VOTING SYSTEMS TASK FORCE

Edwin M. Lee, Mayor

RECOMMENDATIONS ON VOTING SYSTEMS FOR THE CITY AND COUNTY OF SAN FRANCISCO

A Report by the San Francisco Voting Systems Task Force (VSTF)

June 2011

TABLE OF CONTENTS

Section 1:
Introduction and Background

1.1 Mission and Context of the Voting Systems Task Force (VSTF)

In September 2008 the City and County of San Francisco[1] Board of Supervisors established the Voting Systems Task Force to make recommendations to that body about voting systems standards, design, and development.[2] We define our work as follows:

Mission: Our mission is to advise San Francisco on the development and/or acquisition of voting systems that ensure fair and accurate elections, achieve voter intent, and provide for transparency and public auditability of voting systems components and election data.

Scope and Objective: Activities encompass voting systems and related elections issues that affect or are affected by voting systems and voting system acquisition in San Francisco. A "voting system" for this report is defined to be a system of hardware, software, and processes that prepares a ballot and records, collects, transmits, counts, and reports on votes and election results as cast by voters. Included in this definition are the associated reports and audit logs that provide information about management of election data in the system and system use, integrity, administrative access, configuration and configuration changes as well as documentation for support, use and training on use of the system.

Our report contains recommendations, coupled with supporting rationale, for each of the five areas identified by Section 5.405(b) of the Administrative Code:[3]

1. Standards and guidelines to gauge the adequacy, accuracy and trustworthiness of any voting system to be developed or acquired and the adequacy of any vendor or other entity that might develop and deliver such a system;
2. Methods for generating or acquiring designs for a voting system that meets applicable Federal, State, County and City laws, regulations and other requirements and all other goals for the voting system while minimizing system life-cycle costs;
3. Models for development of a voting system including proprietary, disclosed and open source software and hardware approaches and which address aforementioned voting systems requirements and assure a cost effective, highly reliable, maintainable system;

[1]Unless specified individually as "the City" or "the County," San Francisco" will be used to refer to the City and County of San Francisco throughout the remainder of this report.
[2]San Francisco, Calif., Ordinance 268-08 (2008); www.sfbos.org/ftp/uploadedfiles/bdsupvrs/ordinances08/o0268-08.pdf.
[3]San Francisco, Calif., Ordinance 268-08 (2008), page 3, line 4; www.sfbos.org/ftp/uploadedfiles/bdsupvrs/ordinances08/o0268-08.pdf.

4. Business models, including the City and County of San Francisco acting as its own vendor, which promote the transparency of all aspects of design, development, production and the business relationship of all parties associated with production, delivery, implementation and use of the voting system;
5. Any other considerations related to voting systems that will promote public trust in the conduct and results of elections.

Recommendations are presented in five topic areas: election records and post-election audit procedures; balloting systems and services; security; Ranked-Choice Voting; and acquisition strategies.

This report is not intended to be a complete statement of requirements or technical specifications, and it is not an exhaustive study of all topics related to voting systems. Rather, it provides a framework that will guide San Francisco as it seeks its next voting system. A coordinated effort will be needed to establish a policy direction for San Francisco and to support its Department of Elections through a robust and forward-thinking process. We recognize that the City may wish to initiate further investigation of certain topic areas as it considers a direction for San Francisco's next voting system. We recommend that the San Francisco Board of Supervisors establish a body or process to implement the recommendations contained in this report and to maintain steady focus on this issue over coming months and years.

Time Frame for Recommendations: San Francisco is currently under contract with Sequoia Voting Systems (which was acquired by Dominion Voting Systems Corporation in 2010),[4] and has the option to extend that contract through elections in 2013. We have identified several opportunities for improving public confidence in the City's use of Sequoia Voting Systems. However, this report primarily offers guidance regarding San Francisco's next voting system. Our recommendations can be found in Section 2 of this report.

Audiences: Our recommendations are intended to provide guidance to a variety of audiences including the following:

- the San Francisco Board of Supervisors
- the San Francisco Department of Elections
- the San Francisco Elections Commission
- San Francisco voters

[4]Dominion Voting Systems Corporation website (2010), "Dominion Voting Systems Corporation Acquires Assets of Sequoia Voting Systems," (news release); http://www.dominionvoting.com/images/pdfs/DominionAcquiresSequoiaFinal.pdf.

1.2 Background on San Francisco's Current Voting System

On March 31, 2005, the San Francisco Department of Elections (DOE) initiated a Request for Proposals (RFP) process seeking bids for a new voting system (including equipment and services) to collect, count, tabulate, and report votes.[5] In December 2007, the San Francisco Board of Supervisors approved a contract with Sequoia Voting Systems for voting systems/services.[6] Sequoia replaced Elections Systems and Software (ES&S) with which the City had been under contract through the 2007 election cycles.

The Sequoia system was implemented beginning with the February 2008 election. The contract runs through December 2011. The contract with Sequoia Voting Systems for a voting system and associated services is valued at $12,650,233.35 (per Resolution 654-07).[7] The DOE has the option to renew the contract two times, each time for one year and has indicated that it anticipates extending the Sequoia contract through the end of 2013. Were it to do so, the DOE estimates that annual maintenance would be approximately $400,000, and services per election would be approximately $500,000. With three elections scheduled in 2012, the projected cost would be approximately $1.9 million. With one election scheduled in 2013, the projected cost would be approximately $900,000 (two year total: $2.8 million).[8]

Sequoia Voting Systems was acquired by Dominion Voting Systems in June 2010. Subsequently, the City accepted the assignment of the contract from Sequoia to Dominion. In this report, San Francisco's voting system is referred to as the "Sequoia Voting System."

San Franciscan voters use an optical scan voting machine to cast their ballots at the polling place. This machine is a paper-based voting system that optically scans the marks that voters make on a paper ballot and counts the votes electronically when the ballot is inserted. Additionally, each polling place has one Sequoia AVC Edge accessible touchscreen voting machine.[9]

[5]City and County of San Francisco, DOE (6 February 2007),"Contract for New Voting System" (memo from DOE Director John Arntz to Merrick Pascual, Budget Analyst, Board of Supervisors); http://www.sfgov2.org/ftp/uploadedfiles/elections/Announcements/MR2007/20070206.pdf.
[6]City and County of San Francisco government website, "City and Country of San Francisco—NFAMIS Blanket Purchase Order Writing"; http://www.sfgov2.org/Modules/ShowDocument.aspx?documentid=152.
[7]San Francisco Board of Supervisors website, "Resolution No. 65-08," http://www.sfbos.org/ftp/uploadedfiles/bdsupvrs/resolutions08/r0065-08.pdf
[8]San Francisco Department of Elections, e-mail message to Jody Sanford, April 14, 2010.
[9]Nataliya Kuzina, Deputy Director, San Francisco Department of Elections, e-mail message to Jody Sanford, April 19, 2011.

The technical specifications of San Francisco's current voting system are as follows:[10]

Optech Insight Plus
APX Firmware K2.16.080626.1320
HPX Firmware K1.44.080501.1500

Optech 400-C Hardware version 3.00P
WinETP Software version 1.16.6

AVC Edge Model II
Firmware version 5.0.24

WinEDS versions 3.1.012 and 4.0.116B
WinEDS Extended Services 1.0.47
WinEDS Election Reporting Software 4.0.44

Card Activator version 5.0.21

MemoryPack Receiver (MPR) Hardware version D
Firmware version 3.01.080422.0522

1.3 Opportunities Presented by "Next Generation" Voting Systems

John Arntz has been the director of the San Francisco Department of Elections (DOE) since 2002. Under his capable leadership, DOE has conducted well-run elections. Yet, the VSTF believes that there is room to improve the underlying voting system and the procedures that accompany the elections process. We have identified opportunities for improvement in several areas:

- intent of voter and accessibility
- audit and verification procedures
- security
- transparency

These issues exist across the entire election systems landscape. In order to address them, there is a need for innovation in the voting systems marketplace. Yet there are many barriers that limit advancement and prevent new players from entering the market: the regulatory environment at the state and federal level is shifting and cumbersome; developing, testing, and certifying new systems are costly endeavors and time-consuming; the voting systems market is fragmented with multiple jurisdictions and differing systems requirements; and many jurisdictions lack adequate

[10]Nataliya Kuzina, Deputy Director, San Francisco Department of Elections, e-mail message to Jody Sanford, April 19, 2011.

funding to invest in a new system. (The regulatory environment and acquisition marketplace is discussed in detail in Section 2.5: Acquisition Strategies.)

Given these challenges, San Francisco would be prudent (a) to begin immediately considering the characteristics of the voting system it would like to implement after the contract for its current voting system terminates, and (b) to consider the acquisition model it will use to obtain a new system. In fact, the City would be on par with other jurisdictions. Across the nation, jurisdictions are grappling with how to provide elections that are accurate, fair, secure, transparent, and accessible, and with how to evaluate the merits of various systems and acquisition models.

The conversation about next generation voting systems is generating opportunities for collaboration and information sharing. An effort to study future voting systems has been undertaken by at least two other jurisdictions, including the following:

1. County of Los Angeles (California) Voting Systems Assessment Project (VSAP) http://www.lavote.net/voter/VSAP
2. Travis County (Texas) Elections Study Group 2009 http://www.co.travis.tx.us/county_clerk/election/study_group_2009

We acknowledge that the obstacles to progress are significant and that jurisdictions must balance aspiration with pragmatism. However, we believe that San Francisco should be an active participant in the movement toward modernized voting systems, and it should consider a broad range of possibilities regarding the business and partnership model it will pursue to acquire/develop its next voting system.

While a flawless voting system is not attainable, the VSTF members hope that this strategic guidance will help San Francisco implement a voting system that earns the highest level of public confidence.

Section 2: Recommendations

2.1. Election Records and Post-Election Audit Procedures

2.1.1 Introduction

This section concerns the records generated in the course of an election and the procedures for checking records to verify that the election was conducted properly. Comprehensive records and audit procedures are essential for ensuring a correct outcome, deterring fraud, building public confidence in elections, and understanding how to improve the election system. Though there are many types of audits, this section deals only with post-election verification of the results.

2.1.2 Concepts and Definitions

Election records include paper or electronic records at all stages of an election, such as the following:

- **Voter registrations:** lists of the registered voters
- **Election definitions:** lists of the contests and candidates in the election and which groups of voters are eligible to vote in which contest
- **Ballot definitions:** descriptions of the contents and layout of each type of blank ballot
- **Cast vote records (CVRs):** electronic records of the choices that a voter made
- **Audit logs, event logs, and error reports:** timed records of events that took place during the election (e.g. accessing of sensitive information, opening or closing of polls, casting of ballots, granting or revocation of access, actions by election workers)
- **Canvass records:** all records used to reconcile vote totals during the post-election canvass period (period between election night and the date an election is certified), including ballot reconciliation sheets, records establishing chain of custody, and other precinct records
- **Vote counts:** counts of the votes (usually within an election district)
- **Election outcome:** the winning candidate in a contest, or the winning side of a referendum, as determined by the vote counts from all districts
- **Election results:** the final report of overall vote counts and outcomes, including the number of ballots cast, voter registration and turnout percentages, and other election statistics

A **post-election manual tally** (sometimes called a post-election audit) is a procedure conducted after an election to check the vote counts. It is usually performed by dividing the cast ballots into

groups called **audit units**, selecting some fraction of the audit units for a manual count, and checking that the manual counts for each unit match the vote tallies from the election. The California Elections Code, Section 15360,[11] currently requires a manual tally of the ballots from 1% of the precincts.

A **risk-limiting audit** is an audit that ensures a high, pre-specified chance of detecting and correcting an incorrect election outcome. Any auditing procedure that can provide such a guarantee qualifies as a risk-limiting audit. For the purpose of this definition, the correct outcome is the outcome that a full hand count of all the ballots would have produced. Audits can be made risk-limiting by establishing specific criteria under which a full hand count must occur. Typically a risk-limiting audit involves hand-counting a randomly selected sample of the ballots (where the number of ballots to count depends on how close the contest was), comparing the hand-verified results to the vote tallies, and escalating to a full hand count if the error is sufficiently large. For example, to limit the risk of an incorrect outcome to 1%, the sampling procedure and escalation criteria must be chosen such that there is at least a 99% chance of escalating to a full hand count when the outcome is incorrect.

Ranked-Choice Voting (RCV) is an election method in which each voter ranks the candidates and the votes are counted through a multiple-round elimination process. This method is also known as Instant-Runoff Voting or the Alternative Vote. As currently implemented in San Francisco, each voter indicates a first choice, an optional second choice, and an optional third choice for an elected office. In the first round of counting, all ballots are assigned to their first choices. If one candidate now has a majority of the ballots, that candidate wins. If not, the candidate with the least ballots is eliminated; ballots with that candidate as their first choice are then reallocated to their second choice, or set aside as exhausted ballots if there is no second choice. Rounds of counting and elimination repeat—always assigning each ballot to its highest-ranked non-eliminated candidate—until one candidate has a majority of the non-exhausted ballots.

Election Markup Language (EML) is a suite of XML-based data formats for election records, defined by the Organization for Advancement of Structured Information Standards (OASIS). The current version is EML 5.0 and work on EML 6.0 is under way. EML defines several different data formats for different kinds of records; each format is identified by a number.

[11] California Legislative Counsel government website, "Election Code Section 15360"; http://www.leginfo.ca.gov/cgi-bin/displaycode?section=elec&group=15001-16000&file=15360.

2.1.3 Findings

2.1.3.1 Voting System Vulnerabilities

Numerous independent investigations have discovered serious security weaknesses and design errors in widely used electronic voting equipment. Some examples are cited as follows:

- In 2004, four computer security experts examined the source code of a DRE voting machine[12] and found it to be "far below even the most minimal security standards applicable in other contexts."
- In 2006, investigators at Princeton University demonstrated that it is possible to construct a software virus that spreads from voting machine to voting machine—even when the machines are not connected to a network—while altering votes in an undetectable fashion.[13]
- In 2007, a team of reviewers appointed by the California Secretary of State found major security flaws in three of the major brands of voting systems used in California, [14, 15, 16, 17] including vulnerability to infection by a software virus in some cases.
- In 2008, the election system in Humboldt County erroneously deleted 197 ballots.[18]

Voting machines are still perceived as untrustworthy in the public consciousness. The investigations mentioned above were widely publicized, and there continues to be a steady flow of news headlines raising concerns about flaws and reliability problems with voting machines.

Finding 1: It is not safe to rely solely on electronic voting equipment for accurate results.

---

[12]Kohno, Tadayoshi, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach (2004). Analysis of an Electronic Voting System. In *Proceedings of the 2004 IEEE Symposium on Security and Privacy*, pp. 27-40. IEEE Computer Society Press.

[13]Feldman, Ariel J., J. Alex Halderman, Edward W. Felten (2007). "Security Analysis of the Diebold AccuVote-TS Voting Machine." In *Proc. 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT/WOTE '07)*; http://citp.princeton.edu/pub/ts06EVT.pdf.

[14]California Secretary of State Debra Bowen government website, "California Top-to-Bottom Review of Voting Systems" (TTBR); http://www.sos.ca.gov/voting-systems/oversight/top-to-bottom-review.htm.

[15]Calandrino, Joseph A., Ariel J. Feldman, J. Alex Halderman, David Wagner, Harlan Yu, and William P. Zeller (2007a). "Source Code Review of the Diebold Voting System." (report, University of California, Berkeley under contract to the California Secretary of State's TTBR); http://www.sos.ca.gov/voting-systems/oversight/ttbr/diebold-source-public-jul29.pdf.

[16]Inguva, Srinivas, Eric Rescorla, Hovav Shacham, and Dan S. Wallach (2007). "Source Code Review of the Hart InterCivic Voting System." (report, University of California, Berkeley under contract to the California Secretary of State's TTBR); http://www.sos.ca.gov/voting-systems/oversight/ttbr/Hart-source-public.pdf.

[17]Blaze, Matt, Arel Cordero, Sophie Engle, Chris Karlof, Naveen Sastry, Micah Sherr, Till Stegers, and Ka-Ping Yee (2007). "Source Code Review of the Sequoia Voting System." (report, University of California, Berkeley under contract to the California Secretary of State's TTBR); http://www.sos.ca.gov/voting-systems/oversight/ttbr/sequoia-source-public-jul26.pdf.

[18]California Secretary of State Debra Bowen government website, "Report to the Election Assistance Commission Concerning Errors and Deficiencies in Diebold/Premier GEMS Version 1.18.19," (2009). https://www.sos.ca.gov/voting-systems/vendors/premier/sos-humboldt-report-to-eac-03-02-09.pdf.

Finding 2: Public confidence in electronic voting has been diminished by the discoveries of serious flaws in electronic voting systems.

2.1.3.2 Current Auditing Procedures

San Francisco's post-election audit is known as the "1% Manual Tally," in which the ballots from a random selection of precincts are manually counted.[19] The manual counts are checked against machine reports at the precinct level. For speed and accuracy, the contests are counted one at a time; that is, each counting team counts a single contest for an entire precinct, then counts the next contest for the entire precinct, and so on.

We inquired as to the procedure taken when the audit appears to be at variance with the reported election results. When there is a discrepancy of even one vote, the ballots are counted again, with particular attention to counting the ballots as a machine would count them, not as a human would interpret the voter's intent. That is, the audit seeks a way to interpret the ballots that confirms the machine result. If a discrepancy remains after a second count, the audit team fills out a Manual Tally Incident Report, which is reviewed by supervisors in charge of the canvass. There is no formal written procedure for escalating the audit or challenging the election results based on such a discrepancy.

Finding 3: The current post-election audit procedure does not establish a known limit on the risk of an incorrect outcome.

2.1.3.2.1 Auditing Procedures for Non-RCV Contests

For a regular contest, the manual count produces a tally of the number of votes for each candidate. These numbers are then compared directly to the vote counts on the machine report for the precinct. The counting process is quite fast, because the ballots are first sorted into piles (one pile for each candidate), and then each pile is counted. We watched a video of the manual tally for a ballot measure; a member of the team counted the "Yes" pile, speaking "Yes, yes, yes, yes, yes…" at a rate of about two ballots per second.

If this manual tally process were carried out for every precinct, it would give assurance that the counts are correct in every precinct, and thus the totals are correct for the entire election, and thus the outcomes (winners) are also correct. Performing this process for a randomly selected fraction of the precincts therefore verifies the outcome with a known level of confidence. This level of confidence can be calculated, and it depends on how many precincts are checked, the number of ballots, and the margin of victory. A 10% tally provides higher confidence than a 1% tally, and a 100% tally provides complete confidence.

2.1.3.2.2 Auditing Procedures for RCV Contests

For an RCV contest, the team manually counts the first choices, second choices, and third choices separately, as if they were three independent contests, resulting in three counts for each candidate. These are compared directly to the machine report, which also provides vote counts of

[19] San Francisco Department of Elections, SF RCV BDProcedures2009-Final.xls, electronic file.

each RCV contest as though it were three independent contests. Next, the team carries out the RCV elimination process *at the precinct level*. That is, if no candidate has a simple majority of the first-choice votes *in the precinct*, then the candidate with the lowest number of first-choice votes in the precinct is eliminated; those ballots are transferred to piles for their second-choice candidates, and so on.

Since the actual election outcome is determined by elimination based on totals for the entire election, the sequence of candidates eliminated during the manual precinct tally bears no relationship to the actual elimination sequence. Also, checking the three independent totals does not verify the outcome because the outcome depends on which first-choice votes are cast with which second-choice votes—not just how many of each there are. Thus the RCV manual tally process does not verify the outcome of the election (see Appendix A for a detailed example).

Finding 4: The manual tally procedure for RCV contests is significantly more complex than the procedure for non-RCV contests.

Finding 5: The manual tally procedure does not verify the outcome of RCV contests.

2.1.3.3 Alternative Auditing Procedures

2.1.3.3.1 Independent Verification

The deletion of 197 ballots in Humboldt County led to the certification of incorrect results in the November 4, 2008, General Election. The discrepancy went undetected until it was discovered by an audit conducted by the Humboldt County Election Transparency Project.[20] The ballots were scanned with a general-purpose, high-speed office scanner. A pre-imprinter attached to the scanner printed a unique serial number on each ballot before scanning. The resulting scanned images were then counted by an image analysis program called TEVS,[21] written by Mitch Trachtenberg. TEVS is freely available under an open source license and has been developed further since 2008.

Finding 6: An independent verification of an election has been successfully conducted by scanning and counting ballots using ordinary office equipment and free software, and such procedures can be effective at detecting errors in election results.

[20]Humboldt Election Transparency Project, last accessed on June 23, 2011; http://humtp.com/.
[21]Trachtenberg Election Verification System, last accessed on June 23, 2011; http://code.google.com/p/tevs/.

2.1.3.3.2 Risk-limiting Audits

In 2008, Joseph Hall et al. conducted risk-limiting audits of four contests from elections that took place in California's Marin, Yolo, and Santa Cruz counties. The authors reported that "[t]he cost and the time required were modest….There remains room for big gains in efficiency—that is, for reducing the number of ballots that must be counted to confirm an election outcome that is, in fact, correct."[22]

In 2009, risk-limiting audits were performed for two contests in Yolo County, as reported by Philip Stark.[23] In one case, the audit units were batches of between 200 and 600 ballots, and the risk-limiting audit required hand-counting 1,437 ballots—a little more than 11% of the ballots cast. In the other case, the audit units were individual ballots, and the risk-limiting audit required hand-counting only 32 ballots.

Finding 7: Risk-limiting audits have been carried out successfully in California.

We note that several risk-limiting audit methods have been proposed and published in peer-reviewed literature. One notable example is the method proposed in "Super-Simple Simultaneous Single-Ballot Risk-Limiting Audits," [24] which audits all the contests on the ballot at once, requires just one parameter to be calculated by a formula (which needs to be calculated only once before the audit begins), and has a simple method for determining how many ballots to check. However, all the proposed methods so far assume a non-RCV contest: there appear to be no peer-reviewed, published methods for risk-limiting audits of RCV contests.

Finding 8: There is at least one peer-reviewed risk-limiting audit method for non-RCV contests that is practical and straightforward to carry out.

Finding 9: There do not appear to be any peer-reviewed risk-limiting audit methods for RCV contests that have yet been published.

2.1.3.3.3 Ballot-level Auditing

In addition to Stark, other researchers also report that auditing at the individual ballot level dramatically reduces the number of ballots that need to be hand-counted in order to achieve a high degree of confidence. Calandrino et al. (2007b)[25] have proposed a method of ballot-level auditing that uses a machine to mark each ballot with a unique number, so that randomly selected

---

[22]Hall, Joseph Lorenzo, Luke W. Miratrix, Philip B. Stark, Melvin Briones, Elaine Ginnold, Freddie Oakley, Martin Peaden, Gail Pellerin, Tom Stanionis, Tricia Webber (2009). "Implementing Risk-Limiting Post-Election Audits in California"; http://www.usenix.org/event/evtwote09/tech/full_papers/hall.pdf.

[23]Stark, P.B. (2009). "Efficient Post-Election Audits Of Multiple Contests: 2009 California Tests." (Refereed paper presented at the 2009 Conference on Empirical Legal Studies.); http://ssrn.com/abstract=1443314.

[24]Stark, P.B. (2010). "Super-Simple Simultaneous Single-Ballot Risk-Limiting Audits," in the 2010 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE '10); http://www.usenix.org/events/evtwote10/tech/full_papers/Stark.pdf.

[25]Calandrino, Joseph A., J. Alex Halderman, and Edward W. Felten (2007b). "Machine-Assisted Election Auditing"; http://www.usenix.org/events/evt07/tech/full_papers/calandrino/calandrino.pdf.

ballots can be individually retrieved and checked against their corresponding cast vote records. Even without such markings, keeping the ballots stacked in the same order that they were scanned is sufficient to make ballot-level auditing possible.[26] The number of ballots to check depends on the margin of victory; closer contests require more manual checking. Calandrino et al. (2007b) analyzed the statewide contests in the Virginia elections in November 2006 and found that in order to achieve a 99% confidence level of detecting an incorrect outcome, a ballot-level audit would require hand-counting 40 times fewer ballots than a precinct-level audit.

Finding 10: Performing a risk-limiting audit with large audit units (e.g. randomly selecting entire precincts for manual counting) is likely to be more expensive than a 1% manual tally.

Finding 11: Performing a risk-limiting audit at the ballot level (i.e. randomly selecting individual ballots for manual counting) is likely to be considerably cheaper than a 1% manual tally, while providing stronger assurance that the outcome is correct.

2.1.3.3.4 Assembly Bill 2023

We note that California Assembly Bill 2023[27] (AB 2023) authorizes the establishment of a groundbreaking pilot program to conduct risk-limiting audits in "5 or more voluntarily participating counties" during 2011. The program will yield a report to the California Legislature evaluating the effectiveness and efficiency of the audits. We find that the definition of "risk-limiting audit" given in AB 2023 matches the meaning intended in this report.

Finding 12: The AB 2023 pilot program provides a valuable opportunity to conduct officially recognized risk-limiting audits, advance the state of the art in post-election auditing procedures, and achieve higher confidence in election outcomes.

2.1.3.3.5 File Formats

Those who have conducted the aforementioned audits also reported that "[a] great deal of scripting and hand editing was required to make the exported data [from Election Management Systems] useful….Election auditing requires better 'data plumbing' than EMS vendors currently provide….One suitable format is the OASIS Election Markup Language (EML)…."[28]

---

[26]Note: In order to preserve voter anonymity, it is important not to order the ballots in a way that can be correlated with the order in which public records show the voters as having cast their votes.

[27]Official California Legislative Information, "Assembly Bill 2023"; http://www.leginfo.ca.gov/pub/09-10/bill/asm/ab_2001-2050/ab_2023_bill_20100719_chaptered.pdf.

[28]Hall, Joseph Lorenzo, Luke W. Miratrix, Philip B. Stark, Melvin Briones, Elaine Ginnold, Freddie Oakley, Martin Peaden, Gail Pellerin, Tom Stanionis, Tricia Webber (2009). "Implementing Risk-Limiting Post-Election Audits in California"; http://www.usenix.org/event/evtwote09/tech/full_papers/hall.pdf.

Neal McBurnett worked with the Boulder County Elections Division to conduct an audit for the 2008 General Election in Boulder County, Colorado,[29] and reported the following:

- Most of the reports produced by the Hart tally system were poorly specified or hard to parse for auditing.
- The Hart tally system produced an XML report that was usable for auditing, though it still lacked some important information and did not adhere to the EML standard.
- Effective audits are easier and require less hand counting to achieve a similar level of confidence if results are reported in smaller audit units.

Both of these reports point to non-proprietary reporting formats, specifically EML. We are also aware of IEEE P-1622, which is another voting data standard under development with more of a focus on elections in the United States. We have not reviewed the specification for P-1622, as the IEEE P-1622 Working Group's working documents are not freely available on its website. If and when P-1622 is a fully developed, freely available open standard with comparable expressiveness to EML, it may also be a suitable option.

Finding 13: The use of proprietary, vendor-specific data formats increases the difficulty of conducting an audit or forensic investigation.

Finding 14: Election Markup Language is a suitable structured data format for enabling efficient post-election audits.

2.1.3.3.6 End-to-end Verification

Another way to establish confidence in an election is to provide the voters with a way to verify that their own votes were correctly recorded and included in the tally. Voting systems that make this possible are said to offer **end-to-end verification**. At the same time, however, it is important to avoid enabling voters to prove how they voted in such a way that they can sell their votes, and also to avoid enabling voters to fraudulently claim that their votes were misrecorded. Although this is a tricky set of requirements to satisfy all at once, there is a substantial body of research and invention in voting systems that actually do have all of these properties. To cite one example, a system called Scantegrity II[30] allows voters to note confirmation codes for their choices and check those codes against a published list of the codes for all the cast ballots, but it does not allow them to prove to others which candidates those codes represented. The City of Takoma Park, Maryland, used Scantegrity II for its November 2009 election.

Finding 15: There is at least one voting system offering paper-based end-to-end verification that has been used to conduct a real election.

[29]McBurnett, Neal (2008). "Obtaining Batch Reports for Audits from Election Management Systems: Election Audits and the Boulder 2008 Election" National Institute of Standards and Technology; http://www.nist.gov/itl/vote/upload/neal-mcburnett-boulder-paper.pdf.
[30]Scantegrity, last accessed on June 23, 2011; http://www.scantegrity.org/.

2.1.4 Recommendations

Based on the findings above, the VSTF makes the following recommendations. Recommendations 1 through 7 can begin implementation now. Recommendations 8 through 12 concern longer-term or more speculative changes, such as the criteria for San Francisco's next voting system. Below, the phrase "EML or an equivalent open standard" refers to a publicly available, freely licensed format of equivalent expressiveness to EML, established by a vendor-independent national or international technical standards body.

2.1.4.1 Near-term Recommendations

1. Publish all election records on the city's website, redacting records only as necessary to protect the anonymity of each voter's votes and the privacy of each voter's personally identifying information. Give public notice when records are published. Whenever feasible, use EML or an equivalent open standard format for the published records. The VSTF recommends prioritizing these four types of records first:

    a. *Tallies of the vote counts, under-votes, and over-votes from each precinct:* Publish (using EML section 500 or equivalent formats) as soon as possible after each precinct closes its polls. For RCV contests, publish the tallies of each preference level, to the extent that these tallies can be compared against totals published at the polling place in order to verify the correct transfer of ballots to the central election office.

    b. *Text files of cast vote records, which are currently called "ballot image files":* For precinct-scanned ballots, publish as soon as the memory packs are loaded; for centrally scanned ballots, publish as soon as the ballots are centrally scanned. These must be published before any precincts are randomly selected for audits.

    c. *Election definitions:* Publish (using EML section 200 and 600 or equivalent formats) as soon as the Qualified Candidate List and Official Measures List are complete.

    d. *Ballot definition files:* Publish (in the current proprietary format) as soon as ballot layouts are complete. When EML or an equivalent open standard format is used (see Recommendation 7), publish in that format.

2. Correct the audit procedure for RCV contests in such a way that a 100% tally would actually ascertain the outcome. In particular, as recommended by the California Secretary of State, use entire-election totals—not precinct vote totals—to determine which candidates to eliminate.[31]

3. Pursue participation in the post-canvass risk-limiting audit pilot program authorized by California AB 2023.

[31]California Secretary of State Debra Bowen government website. Debra Bowen (2010) "Instant Runoff Voting in Charter Counties and Charter Cities"; http://www.sos.ca.gov/voting-systems/oversight/directives/irv-guidelines.pdf.

4. Define, pilot, and use a ballot-level risk-limiting audit procedure for all non-RCV contests, taking guidance from Hall et al.'s "Implementing Risk-Limiting Post-Election Audits in California"[32] and considering as one option Stark's "Super-Simple Simultaneous Single-Ballot Risk-Limiting Audits." [33]

5. At such time as a peer-reviewed method for risk-limiting audits of RCV contests has been published, define, pilot, and use a ballot-level risk-limiting audit procedure for all RCV contests.

6. Permit academic organizations[34] to publicly request and obtain timely access to all the paper ballots (without any information linking ballots to voter identities) for the sole purpose of digitally scanning the ballots and analyzing the scanned images to independently verify election results,[35] and to publish their findings from such verification.

7. Permit academic organizations to publicly request, obtain, and study machine audit logs from which any information identifying individual voters has been removed, and to publish their findings from such study.

2.1.4.2 Longer-term Recommendations

8. Consider broadening the audience with access in Recommendations 6 and 7 to include other organizations that serve the public interest, or all members of the public, under conditions that limit conflicts of interest, provide full transparency, protect voter privacy, and discourage vote-selling.

---

[32]Hall, Joseph Lorenzo, Luke W. Miratrix, Philip B. Stark, Melvin Briones, Elaine Ginnold, Freddie Oakley, Martin Peaden, Gail Pellerin, Tom Stanionis, Tricia Webber (2009). "Implementing Risk-Limiting Post-Election Audits in California"; http://www.usenix.org/event/evtwote09/tech/full_papers/hall.pdf.

[33]Stark, P.B. (2010). "Super-Simple Simultaneous Single-Ballot Risk-Limiting Audits," in 2010 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE '10); URL: http://www.usenix.org/events/evtwote10/tech/full_papers/Stark.pdf.

[34]Note: Due to the precedent set by the Humboldt County Election Transparency Project, the VSTF finds great potential value in enabling independent parties to scan and analyze the ballots. However, we also recognize that making all ballots available to the public creates concerns about voter privacy and may enable large-scale vote-selling. Because we believe that independent verification is a powerful way to establish voter confidence, we prefer to see short-term action rather than have such action delayed, perhaps indefinitely, by the controversy that the public distribution of ballots would raise. Thus, we propose the compromise of making the ballots available for scanning to academic organizations, under the assumption that such organizations have sufficient reputations and oversight to be trusted not to engage in large-scale vote-selling schemes. We do not intend this recommendation to prohibit members of the public from collaborating with academic organizations to participate in the verification process. In fact, we encourage a publicly transparent process.

[35]By way of example, two such systems are or will become available from TEVSystems (http://www.TEVSystems.com, http://code.google.com/p/tevs/) and the Clear Ballot Group (http://www.ClearBallot.com).

9. Use EML or an equivalent open standard format internally within the Department of Elections as the primary data format for election definitions and results.

10. Announce an acquisition preference for voting systems that facilitate auditing of individual randomly selected ballots, for example, by exporting digital cast vote records, by exporting scanned images of ballots, and/or by printing a unique identifier on each ballot at the time the ballot is scanned in order to associate each physical ballot with its digital cast vote record.

11. Announce support for EML or an equivalent open standard format as a procurement requirement for new voting systems—specifically, as the format for election definitions, results, outcomes, and any reports necessary to support the risk-limiting audit procedure in use.

12. Announce an acquisition preference for voting systems that allow individual voters to verify their cast votes after the election and independently check the vote tally, without enabling voters to sell their votes or fraudulently claim that their votes were miscounted.

2.2 Balloting Systems & Services

2.2.1 Introduction

This section addresses selected issues and opportunities for balloting systems and services, which the VSTF believes are the most important to consider in any next-generation elections administration and voting systems platform. Where possible, this section makes tactical recommendations that can be applied to the current system(s) in place. The majority of this material, however, focuses on recommendations to guide the defining of requirements and specifications for any future voting system acquisition to enhance, extend, or replace what San Francisco currently has deployed.

"Balloting systems and services" as used in this Report refers to those technologies employed for the following uses of secret ballots in a public election: (1) producing ballots prior to an election or on-demand during an election; (2) delivering a ballot to a voter, either in person or remotely for absentee voters; (3) marking a ballot, whether manually marking a paper ballot, digitally marking an electronic ballot, or using digital means to indicate ballot choices that are then represented on a printed ballot; (4) presenting a ballot to be counted, whether remotely or in-person, or presented physically or digitally; and (5) the actual counting of ballots.

The "secret ballot" is used here in recognition that it has been traditionally a term of art within the elections administration community. However, it is important to balance the access to and verifiability of election records (including ballots) with the need to maintain voter privacy. The principal quality of the U.S. election system that guarantees this privacy is perhaps best described more constructively as "ballot anonymity" rather than "ballot secrecy." Ballot anonymity means that voters cannot provably be associated with their vote data. It does not mean that ballots should be kept secret after casting. Incidental recognition of a ballot image or a vote pattern by the voter is probably unavoidable without closing off access in an irrevocable manner. Even so, there are means available to reduce the likelihood that personal identities will be associated with otherwise anonymous records.

Ballot anonymity should be recognized as an essential part of any existing or future voting system. There is concern that coercion and vote buying/selling might occur when specific ballots can be linked to specific voters. (See recent cases of vote buying and selling in Kentucky for an example.)[36] This danger, however, should not be over interpreted in a way that leads to the loss of necessary transparency in the counting of ballots or the verification of counts. At the same time, it is important to consider dangers inherent in selective access to election records (e.g. for officials only).

[36]See http://www.kentucky.com/2010/11/03/1506063/voting-going-smoothly-across-kentucky.html.

2.2.2 Concepts and Definitions

- **Direct-Record Election device (DRE):** a computer-based device that presents a ballot as a series of ballot items; accepts voter selection(s) for each ballot item; provides navigation, help, confirmation and other UI functions; records an electronic ballot that comprises all of a voter's ballot item selections. Some DREs include a voter-verified paper audit trail (VVPAT).
- **Remote Digital Voting:** is a voting method in which marked ballot data is digitally transmitted from voter to election officials, either with or without a paper trail.
- **Uniformed and Overseas Civilian Absentee Voter Act (UOCAVA):**[37] an act of the U.S. Congress that places requirements on states' conduct of elections to include measures to enhance access by (a) military or civilian voters not residing in the U.S. or (b) military voters on service away from their locality of voter registration.
- **Vote By Mail (VBM):** a voting method by which a blank ballot and voter affidavit are sent via postal service to an absentee voter, who is expected to complete both documents and return them via postal or express service, packaged in such a way that the affidavit can be viewed without viewing the marked ballot. Jurisdictions employ a wide variety of methods for packaging, for information required on affidavits, and for validation (if any) of the affidavit sometimes including a signature.
- **Voter-Verified Paper Audit Trail (VVPAT):** a paper-based component of a DRE. Some DREs print a VVPAT for a voter to view and independently verify before casting an electronic ballot. Such VVPATs are removed from view after casts; in some jurisdictions, VVPATs are used for hand-count audits of DRE counts.

A **Ballot Marking Device (BMD)** presents a ballot as a series of ballot items; accepts voter selection(s) for each ballot item; provides navigation, help, confirmation and other user interface functions; records the voter's selections by printing a paper ballot that the voter can cast in the same manner as paper ballots that were marked by hand. Some BMDs print only selection marks (e.g. bubbles) on pre-printed ballots; other BMDs print a complete ballot on a blank sheet(s) of paper.

The **Central Count Optical Scan device (CCOS)** incorporates digital image capture and digital image processing techniques to acquire an image of each sheet of a deck of paper ballots, identify voter marks on the ballot, and interpret each mark as a choice for a particular contest's candidate or choice. The votes from each scanned and counted ballot are tallied to produce vote totals from the set of ballots scanned during a single run of the device. Some CCOS devices retain ballot images and/or individual records of each counted ballot. Some CCOS devices reject ballots with ambiguous marks, while others provide a user interface for election officials to interpret the voter's intent and indicate how an ambiguous mark should be realized and recorded as a vote or non-vote.

[37] Uniformed and Overseas Civilian Absentee Voter Act; http://web.archive.org/web/20080126231627/http://www.fvap.gov/laws/uocavalaw.html.

The **Precinct Count Optical Scan device (PCOS)** is similar to a CCOS device, except that a PCOS device works on individual paper ballots rather than a deck of ballots, and the intervention for ambiguous ballots is to offer the voter (presumed to be present while the ballot is scanned and counted) options to re-try with a new or updated ballot, or to proceed with counting despite ambiguous marks that might result in some of the voter's votes not being counted.

An agency of the U.S. Federal government, **Federal Election Assistance Commission (EAC)** was created by the Help America Vote Act (HAVA) of 2002[38] with the task of assisting state and local election administration organizations in improving their capability to conduct U.S. government elections. The EAC primarily funds state and local election administration organizations, but it also awards research contracts for investigation of election-related matters. The EAC has funded the replacement of voting systems for much of the country, notably including voting systems that meet HAVA mandates for accessibility.

The **Federal Write-In Absentee Ballot (FWAB)** is a paper form that UOCAVA voters may use (a) to fill out an absentee voter affidavit, and (b) to write a list of ballot items and the voter's choice for that ballot item. Use of an FWAB requires that the voter have independent knowledge of the items on the ballot that the voter is entitled to vote. If a voter makes errors in following the instructions for the affidavit, including the State-specific requirements, then local election officials may choose not to count the voter's ballot.

DRE Double Commit refers to a DRE function that creates a risk for disenfranchisement. With some DREs, when a voter casts a ballot, the voter is prompted to confirm that they are finished voting, and then prompted a second time to commit and cast the electronic ballot. The disenfranchisement risk arises in practice because voters sometimes leave the polling place after the first confirmation, but without responding to the prompt for the second confirmation. At that point, the DRE will eventually time-out the voter session and not cast or count the ballot; also, until that time, poll workers have the opportunity to cast the ballot, either as is, or with modifications to the voter's selections.

2.2.3 Findings

2.2.3.1 Ballot Accessibility and Availability

The current state of ballot accessibility and availability issues apply distinctly to three categories of voters:

- **Local In-person Voter:** Voter and ballot information is provided by postal distribution and Web publication of personalized sample ballots that are close facsimiles of the actual paper ballots.

[38]Federal Election Commission, "Help America Vote Act of 2002"; http://www.fec.gov/hava/law_ext.txt.

- **Uniformed and Overseas Voter:** Voter and ballot information as well as the official vote-by-mail blank ballot with an associated attestation document are made available by postal distribution at least and digital means at best to be compliant with Federal MOVE Act regulations.[39]
- **Other Absentee Voters:** Voter and ballot information as well as the official vote-by-mail blank ballot with an associated attestation document are provided by postal distribution. Applications materials for absentee voter status are available by Web download for preparation and return via postal service or in-person delivery. Special needs voters are able to obtain assistance in ballot marking and casting only if they are physically able to make it to a public polling place. These voters' only option is to rely on paper vote-by-mail ballot if they are able.

Finding 1: Voter and ballot accessibility and availability are tailored to different types of voters' needs, but there are still areas that could be improved when voters need assistance completing a ballot (e.g. special-needs voters using vote-by-mail ballots).

2.2.3.1.1 DRE Devices for Special-Needs Voter Ballot Casting

In addition to those issues discussed above, there are issues pertaining to accessibility and usability of the ballot itself.[40] These devices do not produce a durable paper ballot of record equivalent to ballots provided to non-DRE voters. For special-needs voters utilizing DRE-based ballot casting services, there is an increased risk of loss of anonymity via a voter-sequence-correlation privacy exposure. This exposure arises in a scenario where most voters cast a paper ballot—and DREs are typically only used by special-needs voters—in small numbers.[41] Poll workers are capable of recalling or recording by name the sequence of special-needs voters and then communicating that information to staff members who have access to VVPATs or time-stamped audit logs and who can then determine how each DRE voter voted.

Even when the number of DRE voters is not small, privacy exposure can occur in other ways—especially during primaries and other elections with multiple ballot-styles used in a single polling place. The privacy violation risk for the special-needs voter is one example of the importance of the principle that all voters cast a ballot in the same manner, so the ballots of some voters are not erroneously segregated, creating a risk for ballot attribution. This principle supports the use of BMDs so that voters can choose to mark manually or digitally, but the ballot is cast and counted

[39]California Secretary of State Debra Bowen government website (28 January 2010). Memo regarding "Military and Overseas Voter Empowerment Act"; http://www.sos.ca.gov/elections/ccrov/pdf/2010/january/10042cbm.pdf.

[40]See Noel Runyan and Jim Tobias (26 July 2007), "Accessibility Review Report for California Top-to-Bottom Voting Systems Review"; http://www.sos.ca.gov/voting-systems/oversight/ttbr/accessibility-review-report-california-ttb-absolute-final-version16.pdf.

[41]Note: For example, if a few hundred people in a polling place vote on paper and PCOS, and a handful of special-needs voters use a DRE, then poll workers know that the handful of special-needs voters cast that handful of votes. Or, if one person is the only one to vote for a particular party, then poll workers would know who cast that single ballot. However, when BMDs are used (as discussed elsewhere in this Section), voters can choose to mark manually or digitally, but the ballot is cast and counted in the same manner regardless.

the same manner regardless. The advantage of a BMD over a DRE is that a paper ballot is produced for counting, audit, and verification purposes.

Finding 2: DRE devices incur a risk of loss of voter anonymity.

Finding 3: A BMD could provide a record for each ballot.

2.2.3.1.2 Physical Durability of VVPAT Ballots

DRE-voters are disadvantaged in audits or recounts due to the less durable nature of a VVPAT ballot compared to standard paper ballots. Moreover, VVPAT rolls of paper are difficult to count in the case of manual recounts and full recounts.[42]

Three usability limitations should be addressed:

1. The need exists to verify instruction text meets EAC guidelines[43] for plain-language and moderate-level literacy accessibility.
2. The need exists to verify visual aids exist in instruction text.
3. There is likelihood that ballot layout does not meet guidelines of EAC-funded AIGA[44] best practices in ballot design.

Finding 4: VVPAT ballots have questionable limitations in design and physical makeup.

2.2.3.1.3 Other Supportive Rationale

The VSTF also located three areas where improvements in the system could be beneficial to voters.

The State of California historically asserted compliance to the MOVE Act, which is a 45-day advance availability provision by postal distribution means of absentee voter materials for UOCAVA voters. Nevertheless, exploring opportunities to make these materials more readily available by digital means pursuant to the MOVE Act could better serve U.S. overseas and military voters.

Special-needs voters tend to be disenfranchised should their individual situation prevent their ability to travel to a polling place to cast their ballot. Mobile accessible balloting services could provide these voters with a more accessible means to vote.

As an equal protection principle, consistent enfranchisement depends on consistent ballot format and ballot counting procedures. This principle is not currently met in practice because some voters have their votes counted from paper ballots while other voters have their votes counted relying on VVPAT devices. Therefore, aspiring to a single ballot design, layout, and presentation for the ballot of record can achieve the long-term recommendation.

---

[42]For example, see the VVPAT section on this page: http://www.countedascast.com/issues/audits.php.
[43]EAC guidelines, last accessed on June 23, 2011; http://www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx.
[44]See generally: http://www.aiga.org/content.cfm/election-project.

Finding 5: U.S. overseas and military voters could be better served with a digital means of receiving election information and a blank ballot.

Finding 6: Special-needs voters could benefit from mobile accessible balloting services.

Finding 7: Consistent ballot format and counting procedures can help to maintain voter enfranchisement.

2.2.3.2 Ballot Marking and Casting

The current state of ballot marking and casting can be divided into three methods of voting: in-person; remote; and use of the Federal Write-in Absentee Ballot (FWAB).[45]

In-person voting involves the casting and counting of ballots in person in polling places using two methods: (a) precinct optical scan of hand marked ballots, and (b) use of DRE devices for digital casting and counting. In addition to the these methods, some voters are required to vote provisionally by casting a hand-marked paper ballot that is not counted in the polling place but may be counted centrally, if approved by election officials. San Francisco also employs central count optical scan for vote-by-mail ballots and provisional ballots that have been approved by elections officials.

There is significant controversy regarding the security risks of **remote voting**. It is well settled that marking ballots in an uncontrolled environment is vulnerable to fraud and coercion—mostly during transportation (of ballot from voter to election officials) wherein marked ballots are subject to risks that are not present in ballots marked in a controlled environment.

Similarly, in discussing **remote digital voting**, it is well settled that all forms of remote digital voting also share these vulnerabilities, although there is significant controversy regarding scope and scale of the security risks of each form of remote digital voting, as compared with non-digital remote voting. Among the risks specific to remote digital voting are insider technical threat and Internet accessibility of remote digital voting systems to adversaries. Insider technical threat is the expansion of the scope of trusted insiders to include IT operations staff charged with managing remote digital voting systems, as well as anyone who is able to obtain IT operations privileges. Internet accessibility is a necessary consequence of using public networks for communication between remote voters and local election officials; anyone anywhere with Internet access has the ability to target remote digital voting systems in order to carry out the same type of Internet-based attacks that have succeeded against several organizations with security expertise that far exceeds that of any voting system vendor or election jurisdiction—including Google,[46] Adobe, RSA Security,[47] and dozens of other large corporations. With the digital-specific risks, both ballot anonymity and ballot integrity are at risk in many ways that are not applicable to ballots marked in a controlled environment with controlled transportation to election offices facilities.

---

[45]Federal Voting Assistance program website; http://www.fvap.gov/FWAB/fwab-ca.html.
[46] Zetter, Kim (14 January 2010), "Google Hack Attack Was Ultra Sophisticated, New Details Show," *Wired*; http://www.wired.com/threatlevel/2010/01/operation-aurora.
[47]Zetter, Kim (7 June 2011), "RSA Agrees to Replace Security Tokens After Admitting Compromise," *Wired*; http://www.wired.com/threatlevel/2011/06/rsa-replaces-securid-tokens/.

An interesting example was the Okaloosa Distance Balloting Pilot,[48] which used a combination of early-voting center operations, kiosk-style Internet voting in controlled environment, and paper ballot-like voter-verified paper records used for auditing the Internet voting tallies. More recent proposals for digital-enabled kiosk voting have included methods that do not rely on Internet voting techniques. In any event, the concepts of controlled environment and a verifiable paper trail and audit trails have emerged as the top issues wherein any remote voting solution is contemplated.[49, 50]

These issues were highlighted in the Okaloosa report that noted the system is vulnerable to attack by trusted insiders (such as election officials behaving maliciously). Defending against such attacks can be challenging in any voting system. In Scytl's system, Voter Choice Records are pivotal to this defense. Manual counts of the Voter Choice Records, as well as procedural controls on insider access to the system before and during an election, are the only way we have identified to secure the system against insider threats. We also note that an EAC report reported irregularities in the post-election audit of the Voter Choice Records.[51] There are a number of open issues to be resolved, including but not limited to scalability, transparency, and independent testing.

Federal Write-In Absentee Ballot (FWAB) is a method that is approved by a process similar to vote-by-mail process, but it requires manual intervention for counting purposes.

> **Finding 8:** Although all voting methods must be carefully monitored to prevent malicious or negligent events, the use of remote digital voting—especially the digital return of voted electronic ballots with no audited paper ballots—is far too insecure in public elections application for the foreseeable future.

2.2.3.2.1 Other Supportive Rationale

There are several ways to ensure all voters have equal protection and enfranchisement. A single kind of ballot and a single method of counting can be supported along with support for accessibility. As mentioned earlier in this section, a BMD ensures two principles: (a) special-needs voters obtain automated assistance in ballot marking; and (b) all voters have a paper ballot that is consistently counted in the same manner. Ballot image retention can also be used for improved audit and verification. Moreover, CCOS logging capability can provide improved accountability, audit, and verification.

> **Finding 9:** The use a single type of ballot, BMDs, image retention, and CCOS logging can equally protect and enfranchise all voters.

---

[48] Okaloosa Distance Balloting Pilot, last accessed on June 23, 2011; http://election.dos.state.fl.us/voting-systems/pdf/ODBPplanJune_19.pdf.
[49] See http://www.operationbravo.org/documents/NASS%20VP%20Briefing.pdf.
[50] See http://election.dos.state.fl.us/voting-systems/pdf/ODBPplanJune_19.pdf.
[51] See http://www.eac.gov/assets/1/AssetManager/Martha%20Mahoney%20-%20Comment%20on%20Pilot%20Project%20Testing%20and%20Certification.pdf.

2.2.4 Recommendations

2.2.4.1 Ballot Accessibility and Availability

2.2.4.1.1 Near-Term Recommendations

To improve ballot accessibility and availability in the near future, the VSTF offers the following recommendations:

1. Support provisions of the Federal MOVE Act regulations for digital blank ballot distribution.
2. For special-needs San Francisco-based voters who are physically unable to cast their ballot in a polling place, experiment with mobile accessible ballot marking and printing services.
3. Promote the opportunity for San Francisco voters to access voting information online, including sample ballots.
4. Adopt a stronger privacy-enhancing procedure that requires a larger minimum number of voters using the DRE machines in order to reduce the risk of ballot attribution.[52] Enhance poll worker training to stress this procedure and the need to comply with it. Measure compliance, and publish compliance findings, based on polling-place records of number of checked in voters and number of DRE voters.
5. Create, train, and enforce a requirement that the accessible voting system be set up and working (according to specific criteria communicated in poll worker training) before the polling place is opened for general voting at the start of the Election Day.

2.2.4.1.2 Longer-Term Recommendations

We recommend these long-term actions:

6. Extend the intent of the California Election Code Section 15360[53] by requiring the ballot of record be specifically a paper record of uniform style, layout, and presentation consistent with its hand-marked counterpart instead of a paper artifact fulfilled by VVPAT devices.
7. Use paper ballot layout practices and/or tools that follow the EAC guidelines on visual design and plain language, and deliver these benefits to all voters.
8. Rather than providing polling-place disabled access via DREs, instead provide access via the combination of (a) ballot-marking devices for enhanced access to the ballot, and (b) use of the same precinct-count casting method used by voters without special needs. In addition to removing a ballot anonymity threat of DREs, this approach would have additional benefits: lacking the so-called "double-commit issue" of DREs; providing for a digital count for audit purposes; and adhering to the EAC guidelines on visual design and plain language.

[52]See Footnote 41.
[53]California Legislative Counsel government website, "Election Code Section 15360"; http://www.leginfo.ca.gov/cgi-bin/displaycode?section=elec&group=15001-16000&file=15360.

2.2.4.2 Ballot Marking and Casting

2.2.4.2.1 Longer-Term Recommendations

9. The official "ballot of record" should be a paper **artifact** in uniform design, layout, and presentation consistent with its hand-marked counterpart, in order to enable a consistent method of counting, audit, and verification as well as to ensure a consistent method of ballot anonymity.
10. Enhanced access to ballots should be provided by non-tabulating ballot marking devices rather than tabulating DREs.
11. All in-person voters should have the options of either marking paper ballots by hand, or via the use of a ballot-marking device.[54]
12. Encourage voters who use BMDs to review their printed ballots before casting.
13. All optical scanning devices should retain a good-resolution scanned image of each ballot, together with a complete cast-vote record for auditing support.
14. CCOS devices should provide a user interface for election officials to interpret ambiguous ballots as needed—with full logging of every interpretation—and that said logs should be publicly available.
15. If not done so already, provide data to track cases of UOCAVA voters receiving absentee voting materials, but not having a ballot arrive in time to be counted.

[54]Note: In California, the voters do have the choice of using paper ballots or DREs with VVPATS. However, as a policy matter, the use of DREs is discouraged since all votes cast on a DRE with VVPAT must be counted by hand.

2.3 Security

2.3.1 Introduction

Elections security is vital to protect each voter's rights and assure the integrity of election data. Security throughout the election cycle—including use of the voting systems—must be implemented with procedures. Equally important is the security of the voting system's design, engineering, and manufacture—all elements are fundamental in garnering the trust voters must have in the system they are using to cast and count their ballots. Essentially, each voter relies on the soundness of the security of the voting procedures and the use and design of the system to ensure his or her vote is counted. If not, the integrity of elections and the jurisdictions that manage them can be compromised.

Steps must be taken to build and maintain the voter's trust that (a) the digital chain of custody has not been broken and (b) no event has occurred that might affect the integrity of the election data. Unfortunately, for both physical ballots and the voting system, there are opportunities for fraud or error. The VSTF has scrutinized the issue of security and has determined recommendations that may lead to safer and more secure elections.

2.3.2 Concepts and Definitions

When considering voting system security, the vulnerabilities throughout its use in the election cycle must be examined. The following are major parts of the end-to-end election process that must be considered in system and procedural security:

- **Cryptography:** protecting data from theft or alteration by transforming it (encrypting it) into an unreadable format, called cipher text that requires a secret key to decipher (or decrypt) the data back into plain text
- **Ballot Definition**: the description of the ballot for ballot cards and for the digital vote records
- **Logic and Accuracy (L&A) Testing:** pre-election testing of voting system elements and devices to assure that cast votes will be properly recorded in the voting system
- **Vote Capture:** the point at which the voter's intent becomes a digital record, which will ultimately be aggregated with other votes to determine the election result
- **Vote Transmission:** the movement of electronic data to an electronic/digital data store so that all votes for San Francisco can be read by a computer that tabulates the election results
- **Vote Tabulation:** the tallying of ballots to determine the result for each election contest

For paper ballots, the precinct- or central-ballot **optical scanner device** (e.g. Sequoia Eagle and 400C, respectively) translates the marked, paper ballot to a digital record of the vote. When a **direct recording electronic device** (e.g. Sequoia Edge DRE) is used, the digital vote record is created by touching the devices screen to cast a vote that also produces the voter verifiable paper audit trail (VVPAT). In advance of use for an election, all of these machines undergo a L&A test and recalibrated or repaired as needed to assure they are fit for use in the election.

Data can be **sneaker netted** (downloading data to a device that is physically transported to another location and connected to another device for data upload) or may be transmitted electronically over a network. In San Francisco, the data recorded by the precinct optical scanner and the precinct DRE (Sequoia Eagle and Edge respectively) is saved to a removable memory pack that is transported from the precinct to the election center for upload to the central election data store. San Francisco processes vote-by-mail ballots and validated provisional ballots at the election center with a large, fast optical scanning machine (Sequoia 400C) that transmits data to the central data store over a private computer/data network of CCSF.

For contests that are determined by a plurality, this is a matter of summing of the votes to determine passage of a measure or winner of a race. For **Ranked-Choice Voting (RCV)**—when there is no one candidate who received 50% +1 vote as a first choice—computer algorithms are then used to eliminate candidates and redistribute votes where needed for the voter's second- or third-choice candidate.[55]

2.3.3 Findings

Without proper system security, handling of physical ballots can be open to fraud and error; however, malicious manipulation or negligent management of an electronic version of ballot data can be executed in greater volume, be more precise in intended impact, and be harder to detect. Thus, the level of security in voting systems is essential to assuring an accurate, correct election outcome and in garnering public trust in the election outcome. Effective procedural measures must be implemented throughout the election process to bolster security and to detect issues. A voting system that is designed with security—which is integrated into all of its elements (hardware, software, firmware, data, and network)—that supports effective security procedures will improve voter confidence in the system and election outcome. A system that is designed in concert with effective security procedure can reduce the cost of manual procedures required for security assurance of a system that has poor system security.

Generally, the focus of voting system security is on preventing malicious or negligent events that cause corrupt or inaccurate voting data or otherwise disrupt the ability for a jurisdiction to obtain an accurate election result from its election system. Unfortunately, the jurisdiction conducting an election cannot rely solely on preventive security measures because a completely invulnerable system is impossible to construct. Thus, the review and audit of the election and system information are essential procedures in (a) providing the assurance that security measures were successful or (b) determining that events had transpired that somehow compromised the system. Only with this step is the security regimen complete.

> **Finding 1:** Security must be considered in every feature of a voting system to ensure voter confidence.

> **Finding 2:** A voting system that is designed to be highly secure and designed in concert with security procedures can reduce the cost of security assurance.

[55] See "Section 2: Election Records and Post-Election Audit Procedures" for a more detailed definition of RCVs.

2.3.3.1 San Francisco's Current Voting System: Existing Security Issues and Mitigation

2.3.3.1.1 San Francisco's Procurement Action and Voting System Security Concerns

In 2002, the Federal government mandated a modernization of voting systems with the enactment of the Help America Vote Act (HAVA); funds were allocated for implementation of this mandate.[56] HAVA was timely law for San Francisco, which needed to replace an aging voting system for which its maintenance contract was about to expire. As detailed in the Introduction of this report, San Francisco issued a Request for Proposal (RFP)[57] for the procurement of a new voting system in May 2005. The RFP consisted of an Introduction and 15 appendices that totaled 197 pages. Appendix E "Design, Fabrication and Performance Requirements" (25 pages) contains all requirements, including security. This was not due to disinterest on the part of San Francisco or its Department. of Elections (DOE) on the importance of security, but it does reflect the reliance on the vendor and other agencies to detect and correct security flaws.

The systems that could be implemented to satisfy HAVA requirements and were certified for both Federal and California elections were few. Only two vendors responded to the San Francisco's RFP: Sequoia Voting Systems and ES&S. Public objections to the vendors—which were primarily rooted in transparency and security concerns—stalled execution of the contract for 15 months. However, because no other certified voting systems were available and no viable alternatives were emerging, San Francisco proceeded with the Sequoia procurement. From the standpoint of DOE, this was the prudent course of action: (a) it would bring the DOE into compliance with Federal law, and (b) it would serve its operational needs. Any additional consideration of security was unnecessary and superfluous to fulfillment of its legal obligations under HAVA and support to its operational mission.

2.3.3.1.2 Top-to-Bottom Review

In January 2007, Debra Bowen was sworn in as the California Secretary of State (CA SoS); on that day, she reiterated her campaign promise to assure transparency in the voting systems used in California.[58] She created a project known at the "Top-to-Bottom Review" (TTBR)[59] of the voting systems certified for use in California. The TTBR consisted of a review of software, accessibility, documentation, and a security evaluation. It eventually evidenced many security issues within California's voting systems, including the Sequoia system procured by San Francisco. Security issues were found with all systems that were tested, but we here focus on the Sequoia System used in San Francisco to provide some relevant and insightful specifics on

[56]Federal Election Commission, "Help America Vote Act of 2002," http://www.fec.gov/hava/law_ext.txt.
[57]City and County of San Francisco government website, "RFP," (VSTF page, Appendix E) http://www.sfgov2.org/index.aspx?page=1869.
[58]California Secretary of State Debra Bowen government website, "Secretary of State Debra Bowen, Inaugural Speech" (Monday, January 8, 2007); http://www.sos.ca.gov/bowen_event/inaugural_speech.pdf.
[59]California Secretary of State Debra Bowen government website, "Top-to-Bottom Review"; http://www.sos.ca.gov/voting-systems/oversight/top-to-bottom-review.htm.

security flaws of existing voting systems. The "Source Code Review of the Sequoia Voting System" of the TTBR's Executive Summary[60] pinpointed serious security issues concerning data integrity, cryptography, access control, and software engineering.

2.3.3.1.2.1 Data Integrity Flaws

The review discussed how the Sequoia system "lacked effective safeguards against corrupted or malicious data" that was injected into removable media. This was a particular issue with the devices used by polls workers and other temporary staff with limited authority.

> **Finding 3:** The Sequoia voting system's lacked effective safeguards against corrupted or malicious data into removable data recording media.

2.3.3.1.2.2 Cryptography Problems

The review also stated that many of the security features of the Sequoia system—particularly "those that protect the integrity of the precinct results"—employed cryptography. Every case that the TTBR examined proved how simple it was to circumvent the cryptography. As the review explained, many cryptography functions are not implemented correctly, are based on weak and flawed algorithms, or are used in an ineffective or insecure manner. Because of these issues, "virtually all cryptographic key material is permanently hardcoded into the system" and identical in all of the hardware that was shipped off to other jurisdictions. In short, a person who is able to hack into a similar hardware—within or outside of California—can then extract and obtain the secret cryptographic key that were initially created to protect elections throughout every California county that employs that system.

> **Finding 4:** Sequoia's cryptography was poorly implemented, hard coded into the system, and identical in all of the Sequoia systems used throughout California.

2.3.3.1.2.3 Access Control and Security Mechanisms Issues

The TTBR also discovered issues with access control and other computer security mechanisms that were easily circumvented—despite being designed to protect against "unauthorized use of central vote counting computers and polling place equipment." The WinEDS back-up system was designed to be used for ballot preparation, voting machine configuration, absentee ballot processing, and post-election vote counting. However, its security features and audit logs were found to be ineffective against "inside attackers" who may try to gain access to the WinEDS computers or the network to which these computers are attached.

> **Finding 5:** The security features and audit logs of the WinEDS back-up system could have been easily comprised by insiders.

---

[60]Blaze, Matt, Arel Cordero, Sophie Engle, Chris Karlof, Naveen Sastry, Micah Sherr, Till Stegers, and Ka-Ping Yee (2007). "Source Code Review of the Sequoia Voting System," p. 2 (report, University of California, Berkeley under contract to the California Secretary of State's TTBR); http://www.sos.ca.gov/voting-systems/oversight/ttbr/sequoia-source-public-jul26.pdf.

2.3.3.1.2.4 Software Engineering Weaknesses

The software engineering of the Sequoia voting system was also found at fault by the TTBR. According to the review, the software contained numerous programming errors, many of which had the "high potential to introduce or exacerbate security weaknesses." Basically, the software did not reflect "defensive software engineering practices normally associated with high-assurance critical systems." The review also pointed out that there were many examples of poor or absent error and exception handling and that there were also many cases where the software behavior did not match its corresponding comments and documentation. Some of the problems were the root of the many of the issues the review identified, and even the problems discovered in the software that were not specific to "an obvious vulnerability identified," the number of errors reduced the review's "overall confidence in the soundness of the system as a whole."

> **Finding 6:** The software for the Sequoia voting system contained serious programming errors that reduced the overall trust in the reliability of the voting system.

2.3.3.1.2.5 "Red Team" Security Testing

The CA SoS's security group "acted as a 'Red Team' [penetration testers] and performed a series of security tests of both the hardware and the software,"[61] concluding that—although there was not sufficient time to perform a complete evaluation of the Sequoia voting system—the number of serious security issues that were exposed was cause for concern. Essentially, a determined hacker could modify or invalidate the results of an election. The review impressed that several types of attacks could be launched without any knowledge of the source code. In fact, the Red Team was able to analyze the Edge's firmware binary representation and extend the firmware by using binary patching. This technique allowed them to create a "'debugging' version of the firmware, as well as several different 'malicious' versions"; again, access to the source code to implement these attacks was not necessary.

> **Finding 7:** Access to the source code was not necessary to attack the hardware and software of the voting system.

> **Finding 8:** Public concern over DOE's procurement of the Sequoia Voting Systems was not unfounded.

[61] Computer Security Group (2007). "Security Evaluation of the Sequoia Voting System Public Report," Dept. of Computer Science, University of California, Santa Barbara; http://www.sos.ca.gov/voting-systems/oversight/ttbr/red-sequoia.pdf.

2.3.3.1.3 Security Mitigations Measures Required for Use of the Sequoia Voting System

As a result of the TTBR's findings, on 25 October 2007 SoS Bowen issued the "Withdrawal of Approval of Sequoia Voting Systems, Inc."[62] (updated version issued 1 October 2009)—a document that also provides the requirements needed for re-approval of the system. The result was the generation of the "Optech Insight, AVC Edge 5.0, & Optech 400C California Procedures,"[63] deemed the "Sequoia 4.0 Approved Use Procedures" that allowed conditional re-approval of the system and—with implementation of these procedures—the use of the system in San Francisco.

San Francisco and Sequoia have implemented the mitigation plans approved by the CA SoS. San Francisco DOE maintains a Voting System Security Plan[64] that addresses policies, practices, and procedures for voting system security and that addresses specific requirements for continued approval for use of Sequoia by the California Secretary of State.

> **Finding 9:** The public interest would be served by raising awareness of (a) the Sequoia system vulnerabilities identified in the TTBR, (b) the mitigation measures prescribed by the CA SoS, and (c) the procedures that implement these measures in San Francisco.

2.3.3.2 Current Voting System Security Posture

Based on optical scanning of paper ballots, the fundamental security posture of San Francisco's existing counting methods consists of (1) implementing practices, policies and procedures to meet legal requirements for security, and (2) validation of machine counts by conducting partial hand counts of the vote a technology independent manner as required by California Election Law. The security practices and requirements include reducing or eliminating exposure to attack points such as connections to wireless devices or the Internet as well as using tamper-evident seals, signature checks, and other chain-of-custody procedures that increase the chances of detecting errors or tampering.

"Technology independent" validation (as the phrase applies in this section of the Report) means that vote counts and election results are not produced by the sole reliance on the potentially fallible software and hardware of a voting system, but instead they are produced by a combination of the following:

1. Machine count of virtually 100 percent[65] of paper ballots

---

[62]California Secretary of State Debra Bowen government website, "Withdrawal of Approval of Sequoia Voting Systems, Inc., WinEDS v 3.1.012/AVC Edge/Insight/Optech 400-C DRE & Optical Scan Voting System And Conditional Re-approval of Use of Sequoia Voting Systems, Inc., WinEDS v 3.1.012/AVC Edge/Insight/Optech 400-C DRE & Optical Scan Voting System (December 31, 2009 Revision); http://www.sos.ca.gov/voting-systems/vendors/sequoia/sequoia-31012-revision-1209.pdf.

[63]Optech Insight (August 2008), "AVC Edge 5.0, & Optech 400C California Procedures," (document version 3.03); http://www.sos.ca.gov/voting-systems/vendors/use-procedures/sequoia-use-procedures.pdf.

[64]City and County of San Francisco government website, "VSTF Voting System Security Plan"; http://www.sfgov2.org/ftp/uploadedfiles/VotingSystemsTaskForce/VotingSystemSecurityPlan.pdf.

[65]Note: If Federal Write-in Absentee Ballots (FWAB) are cast, they must be hand counted.

2. Audit of the machine counts via hand-count of a randomly selected subset of the machine-counted ballots[66]

The audit procedure is intended to detect discrepancies in the vote count as tabulated by the voting system versus a hand count of the ballot of record. This procedure should audit a statistically significant sample relative to the number of races and voters, and it should provide a threshold to expand the scope of the audit in the event that significant variances are detected.

As already discussed with respect to security, the audit approach is a forensic method for "detection of errors" and could only discover exploitation of security vulnerabilities with secondary investigation. "Prevention of errors" by exploitation of security vulnerabilities means seeking to create a secure or trustworthy system. However, a perfectly secure system is an impossible goal because all software is potentially fallible.

Finding 10: Basic, prudent security measures are already in practice including but not limited to (a) keeping voting systems components disconnected from public networks, and (b) checking the integrity of device firmware and/or software on voting systems components through pre-election L&A tests.

2.3.3.3 Security for San Francisco's Future Voting Systems

2.3.3.3.1 Comprehensive Voting System Security Examination Not Attempted by VSTF

The VSTF did not attempt a comprehensive examination of information security as it applies to voting systems. The threefold reasoning for this became clear during the course of our research:

1. The state of the voting systems industry is bleak: only two major vendors remain, controlling some 87% of U.S. voting systems in use, with a few smaller vendors serving small pockets of opportunity.
2. Voting technology experts concur that future voting systems design will require a wholesale change in the technology model as well as testing and certification methods and requirements for Federal certification in order for these systems to increase accuracy, transparency, verification, security, and, above all, the voters' trust.
3. The prospective fourth version of the NIST/US EAC Voluntary Voting System Guidelines (VVSG)—which provides the most extensive set of voting system requirements, including both specifications and procedures for security—was expected to be released in 2009, but it has yet to be adopted in a final form.

Finding 11: The VSTF found with regard to voting systems security considerations that a more focused study by more qualified security experts is necessary.

[66]Note: Precinct cast ballots on the Sequoia Edge Direct Recording Electronic (aka DRE) device do not produce a paper record that is machine read. Instead, the vote data is recorded directly to the memory pack that is then transported to a central location and loaded into the main tabulator along with the memory pack from the Sequoia Eagle Optical Scan device. The DRE does produce a paper tape record of the voter's selection by contest (Voter Verified Paper Audit Trail, aka VVPAT). This paper tape record can be used for audit purposes.

2.3.4 Recommendations

2.3.4.1 Security Mitigations Measures Required for Use of the Sequoia Voting System

Accordingly, this Report recommends increased transparency of and communication about San Francisco's implementation of the CA SoS's-mandated mitigations. Specifically the City should create an online resource to complement voter information resources that describe the current system, features, and functions, complete with a walk-through of the steps taken to comply with the CA SoS mandates for the current voting system.

2.3.4.2 Near- to Mid-term Recommendations

Beyond the immediate security concerns specific to San Francisco's current voting system, there are also broader concerns about information security of voting systems. The Report's near- to mid-term recommendations are that San Francisco should increase (a) public awareness and education of the security posture of computer-based vote counting, and (b) transparency of operations with regard to this posture.

2.3.4.3 The Current Voting System Security Posture

Many basic security posture measures are specified as TTBR mitigations, L&A testing practices, and post-election operations reviews. With that in mind, in the interim period between the current state of San Francisco's voting system and any future system to be acquired, the Report advocates the following recommendations:

1. San Francisco should further public trust by increasing communication of the basic points of the security posture and, in particular, by impressing upon the voter that—
    a. The creation of a perfectly secure voting system software is impossible;
    b. Manual audits can provide assurance of a clean and accurate election, thus minimizing the voters' focus on the correctness and integrity of software.
2. San Francisco should continue to maintain the existing practices of L&A testing and TTBR mitigation.
3. San Francisco should increase the operational transparency and adequacy thresholds of statistical audit practices to include the following:
    a. Greater information on and availability of audit results;
    b. Voter education about auditing and results through online resources that complement existing voter information services.

San Francisco should consider various options for increasing the scope of audits beyond the minimum requirements of California Election Law. (See Section 2.1: Election Records and Post-Election Audit Procedures for further discussion and recommendations on this topic.)

2.3.4.4 Security for San Francisco's Future Voting Systems

Accordingly, this Report's overarching recommendation with regard to voting system security is that San Francisco collaborate with or create a new, highly qualified, agile team of 4-6 computer systems scientists to develop a set of guidelines for security aspects of any future voting system to be acquired.

For a procured system, these guidelines should comprise new security requirements to be incorporated into any future RFPs to be responded to by any provider of voting systems to San Francisco. Should San Francisco proceed with a decision to make a system to their requirements, these guidelines should be further developed to become requirements that are incorporated into overall systems design.

This new "Security Guidelines Team" could be a new Task Force or simply collaboration with both academia and computer industry professionals outside of the voting systems industry on a consultative basis. It is crucial, though, that these team members have demonstrated domain expertise in elections technology and related information security matters.[67]

2.3.4.5 Longer-Term Recommendations

Aside from assembling a team of digital security experts to develop RFP guidelines for future voting systems, this Report suggests several features that can support increased voting systems security and elections process integrity (many of which are discussed elsewhere in this Report):

4. Assuring a system that allows for hand marking and machine-assisted creation of marked paper ballots of like media versus providing VVPAT for ballots cast by voters with requirements for enhanced access
5. Continuing the use of precinct-count optical scan for in-person cast ballots and central-count optical scan for absentee and provisional ballots
6. Providing digital images of each counted ballot, with a cast-vote record for each that would be made available for examination
7. Establishing strong protections to assure that all actions that change or update the system are known and that only approved software and hardware are implemented and used in an election with documented, approved change management procedures during an update and deployment of the system
    a. Voting system capabilities for strong authentication, access, and logging of system events and operator actions with notification and audit procedures that assure only authorized access and approved actions were taken in any part of the system

[67]Note: By way of example, but not limitation, three example sources of domain experts include: (a) the California Institute of Technology and Massachusetts Institute of Technology joint project known as the CalTech/MIT Voting Project (see http://vote.caltech.edu/drupal/); (b) ACCURATE: A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections, the organization involved with the TTBR (see http://accurate-voting.org/); and (c) The OSDV Foundation's TrustTheVote Project (see http://www.osdv.org and http://www.trustthevote.org).

b. Logging that should involve actions executed with respect to the system hardware and software and election data, including any change to vote records, such as resolution of under-votes, over-votes, and identification and recording of write-ins

8. Utilizing election management system features and reporting system features for publication of ballot definition data and vote count data as recorded by counting devices.
9. Using common data formats to facilitate publication of such data mentioned above
10. Establishing features related to voting system verification loops, testing practices, and transparency of records of such practices, including (but not limited to) the following:
    a. Straightforward and easily repeatable measures for testing software integrity of voting system components
    b. Election management system features and reporting system features for recording and publishing both components of and results of L&A testing (e.g. test decks and test-count results)
11. Providing a well-documented system that can be maintained and operated with commonly and widely available skill sets (versus vendor dependence that is due to proprietary elements and non-disclosure of system technology)
12. Maintaining transparency throughout the system hardware, firmware and software life-cycle including system design, engineering, and manufacture as well as data formats, encryption and communications protocols, and network security requirements
13. Having the ability to validate only authorized software used to execute the election in the system

These capabilities and features should also be considerations of the proposed Security Guidelines Team for when those team members prepare a set of security guidelines for future RFP and competitive vendor bidding.

2.4 Ranked-Choice Voting

2.4.1 Introduction

Ranked-Choice Voting has been the law in San Francisco since 2002. In March of that year, San Franciscans passed Proposition A,[68] amending the City Charter to make Instant-Runoff Voting (IRV)—commonly referred to as Ranked-Choice Voting (RCV)—the method of electing Mayor, Sheriff, District Attorney, City Attorney, Treasurer, Assessor-Recorder, Public Defender, and members of the Board of Supervisors. This was codified in the San Francisco Charter as Article XIII, Section 13.102.[69] Federal and California State provisional certifications of the required changes to San Francisco's then current Elections Systems and Software (ES&S) voting system were obtained by April 2004, and this method was first used in November 2004 to elect seven supervisors.[70] RCV has also been implemented by more than a dozen other U.S. cities—including three in the Bay Area (Berkeley, Oakland, and San Leandro)—and some States for military and overseas voters; it is also in use in a number of other countries.[71,72]

RCV is existing law in San Francisco. While there remains public debate about RCV as a voting method, the VSTF has assumed its use in San Francisco as a given, and thus we have limited its examination to certain aspects of RCV implementation in San Francisco that relate to voting systems and public understanding of the election process.

2.4.2 Concepts and Definitions

- **Ranked-Choice Voting (RCV):** allows the voter to make multiple selections in a single race in an order of preference. As currently implemented in San Francisco, voters are allowed to vote for three choices among the candidates in an RCV race in a ranked order of first choice, second choice, and third choice.
- **RCV Algorithm:** determines the RCV winner by tabulating votes in a series of rounds. The first round of tabulation counts votes for the first choices in a race. If the top vote getting candidate also has a majority of the votes, that candidate is declared the winner. If no candidate has a majority, then the candidate with the fewest first-choice votes is eliminated from the race. A new round of vote tabulation is then performed in which each vote that had counted for an eliminated candidate is transferred to that ballot's most preferred candidate who remains in the race and the votes are again tallied to see if the top vote getting candidate has a majority of votes. If so, that candidate is declared the

[68]For complete text of Proposition A, see http://www.smartvoter.org/2002/03/05/ca/sf/prop/A/.
[69]For complete text of Section 13.102—Instant Runoff Elections, see http://library.municode.com/index.aspx?clientId=14130&stateId=5&stateName=California.
[70]Fair Vote: The Center for Voting and Democracy website, "San Francisco Successfully Uses Ranked Choice Voting for Citywide Elections, Nov. 2005"; http://www.sfrcv.com.
[71]Fair Vote The Center for Voting and Democracy, "Where Instant Runoff Is Used"; http://www.fairvote.org/where-instant-runoff-is-used.
[72]*Wikipedia*, s.v. "Instant-runoff voting, Global Use," last modified 12 June 2011; http://en.wikipedia.org/wiki/Instant-runoff_voting#Global_use.

winner. If not, subsequent rounds of elimination and transfer are performed until a winner is determined.

- **Continuing and Exhausted Ballots**: A ballot is "continuing" if after a round of elimination the ballot has valid marked choices for a candidate who remains in the race. A ballot is "exhausted" if after an elimination round the ballot does not have marked choices for a candidate who remains in the race.

2.4.3 Findings

2.4.3.1 Public Understanding of RCV

In San Francisco's November 2010 elections there were contests for five County Supervisor seats that were RCV races as called for in the City Charter. In two of these contests, District 2 and 10, the ultimate winner did not receive the most first-choice votes and thus were not the front runners in the first RCV round. This also happened in Oakland's mayoral RCV race. All of these races were competitive and close. District 10 race was perhaps most exceptional. There were 21 candidates listed on the ballot. In a race where nearly 17,808 ballots were cast, there was only a 181 vote spread between the top five first-choice vote getting candidates. The winning candidate had placed third when first-choice votes were tallied in the first RCV round.

Since the November 2010 election cycle various sources—press accounts as well as statements from candidates and other organizations—have scrutinized the RCV elections process and outcome. Some are positive stating that RCV worked as expected and proved its benefits while others are critical claiming the method is undemocratic, or that RCV delivers surprise outcomes that voters do not understand.[73]

The San Francisco Department of Elections (DOE) is required by the City Charter Article XIII Section 13.102(g) to "conduct a voter education campaign to familiarize voters with the ranked-choice…method of voting." The DOE developed a training plan in advance of the first RCV election in November of 2004.[74] This has been a significant effort that produced hard copy and on-line educational materials on the RCV voting method and over 700 outreach events coordinated with 11 community-based organizations.[75] A study conducted by San Francisco State University after the November 2004 election concluded that 87% of voters understood

[73]The following is an article that is representative of various perspectives: Zusha Elinson and Gerry Shih (11 November 2010), "The Winning Strategy in Oakland: Concentrate on Being 2nd or 3rd Choice"; http://www.nytimes.com/2010/11/12/us/politics/12bcvoting.html.

[74]Department of Elections Ranked Choice Voting Public Education Plan November 2, 2004 Consolidated General Election, http://politicalreform.newamerica.net/files/San%20Francisco%20Dept%20of%20Elections%20RCV%20Education%20Outreach%20Plan.pdf.

[75]California Secretary of State Debra Bowen government website, "Implementation of Ranked-Choice Voting: The City and County of San Francisco: November 2, 2004 Municipal Election" (p. 4); http://www.sos.ca.gov/voting-systems/vendors/ess/rcv-final-report.pdf.

RCV "fairly well" or "perfectly well."[76] Though this indicates a high degree of understanding of the process among most voters, that 13 % of voters had a lower understanding of the voting system is significant; this group tended to be (1) lower income, minority voters and (2) those who have a lower incidence of voting. In a considerably less exhaustive but more recent study by the San Francisco Chamber of Commerce "55 percent of voters say they are unsure whether or not their vote is counted if their first, second and third choice candidates are eliminated."[77]

The voter education materials do still exist and can be found on the DOE's website. The level of outreach and educational activity on RCV has not been at the levels they were in 2004.

Finding 1: Public understanding of the RCV election process may have declined since the initial RCV education campaign starting in 2004.

2.4.3.2 Reporting Preliminary Early Election Results

Once votes are cast and captured in the election system as data, they are gathered into the central database to determine the election outcome. For RCV races, the software and algorithms for tabulating the election result are more complex than for elections where the outcome is determined by simply summing the votes of the choices on the ballot. This may contribute to a perception of some voters that they do not understand how RCV works. On the other hand, computerization of the election process has made it easier to frequently produce preliminary election results, and San Francisco DOE has set a very high standard for its frequency of publishing preliminary election results. The DOE's schedule of results reporting for the 2 November 2010 election was the following:[78]

- **Election Night:** Preliminary results for early return, pre-processed vote-by-mail ballots and precinct-counted ballots. The first preliminary results are reported approximately 45 minutes after the close of polls, and updates are reported approximately every half-hour to an hour until midnight. For RCV contests, only first-choice totals are reported.
- **Subsequent Days:** Every day in which new votes are processed, the Department will release updated results until all ballots have been counted and the results are certified.
- **Preliminary Ranked-Choice Results:** Release of preliminary results represent how ranked-choice voting plays out on only the votes counted to date. The first of these preliminary RCV results are released on the Friday after Election Day.

[76]Public Research Institute website (December 2004), "An Assessment of Ranked-Choice Voting in the San Francisco 2004 Election: Preliminary Report" (p. 9); http://pri.sfsu.edu/reports/SFSU-PRI%20Ranked%20Choice%20Voting%20Preliminary%20Report.pdf.
[77]San Francisco Chamber of Commerce (February 2011), "2011 City Beat Poll Results"; http://www.sfchamber.com/2011CityBeatPoll/2011pollresults.pdf.
[78]City and County of San Francisco Department of Elections (November 2010), "Schedule of Results Reporting for November 2, 2010 Consolidated General Election"; http://www.sfelections.org/ec/?m=201011.

Release of results with this frequency is a good practice for transparency. However transparency is reduced by not reporting the preliminary results with the full RCV algorithm applied, involving eliminations and transfers and the detail cast vote records on election night or with every daily update. It should be noted that in San Francisco's first RCV election in November 2004, the DOE had planned to produce a "preliminary and initial RCV Algorithm report the day after the election at 4:00 p.m. as well as up to three times a week until results were final."[79] However, during the first attempt to apply "the RCV algorithm, ES&S [the voting system vendor] realized the system was not tabulating all of the processed ballots and could not produce complete preliminary RCV results."[80] ES&S attributed the issue to a software limitation which was removed and by "that Friday, ES&S isolated and removed this particular limitation on the software."[81] DOE has continued to adhere to this practice of producing the first result with the full RCV algorithm on the Friday after the election with the Sequoia voting system.

As seen in November 2010 RCV contests, second and third choices have a significant effect on the outcome of an RCV contest. Not producing results with the full algorithm applied could contribute to a perception on the part of the public that they do not understand RCV. Timely disclosure of preliminary results with the full RCV algorithm applied will improve transparency and give the public a better understanding of the ultimate election result. It is also important for public monitoring of elections. Full reporting of RCV results avoids reliance on potentially misleading vote totals based only on first choices.

Finally, a substantial area of findings and recommendations in this report is in Election Records and Post-Election Audit Procedures (see Section 2.1). Early release of election results with a fully run RCV algorithm is complementary to improved audit procedures.

> **Finding 2:** The Department of Elections has a good practice of frequently releasing preliminary vote counts, but it does not apply RCV algorithms at each release. And this may contribute to a perception of lack of understanding and/or transparency in the RCV election process.

2.4.3.3 Three-Choice Limit

San Francisco Charter Section 13.102(b)[82] states that:

> The ballot shall allow voters to rank a number of choices in order of preference equal to the total number of candidates for each office;

[79]California Secretary of State Debra Bowen government website, "Implementation of Ranked-Choice Voting: The City and County of San Francisco: November 2, 2004 Municipal Election" (p. 8); http://www.sos.ca.gov/voting-systems/vendors/ess/rcv-final-report.pdf.
[80]Ibid, p. 8.
[81]Ibid, p. 8.
[82]San Francisco, Calif., Charter, Article XIII, Section 13.102(b).

It is clear that the intent is to allow the voter to be afforded the opportunity to rank all candidates in a race, but the same passage goes on to state:

> …provided, however, if the voting system, vote tabulation system or similar or related equipment used by the City and County cannot feasibly accommodate choices equal to the total number of candidates running for each office, then the Director of Elections may limit the number of choices a voter may rank to no fewer than three.

Thus, three choices is the minimum allowed, but this limitation should only be imposed if the voting system is not able to accommodate more choices. San Francisco has been using RCV with this minimum level of capability due to San Francisco's Sequoia voting system limitations.

However, the law says the voter should be able to rank all candidates for good reasons: the three-choice limit imposed by the voting system limits voters full expression. In a recent court decision, the U.S. 9th Circuit Court of Appeals concluded:

> If aspects of the City's restricted IRV scheme…impose any burdens on the voters' rights to vote, they are minimal at best. Moreover, the City has advanced valid, sufficiently-important interests to justify using the system.[83]

So although San Francisco's current implementation of RCV does not violate the voters' constitutional rights, "restricted IRV" does limit the voter's ability to fully express their choices in an RCV election. In the case that voters would want to express more than three choices in an RCV election and that the ballot and voting system could accommodate those choices (which is the clear intent of Section 13.102[b] of the City Charter), the ability of voters to fully express those choices could materially affect the outcome of an RCV election.

The November 2010 District 10 Supervisor election is an instructive example. In this race 17,808 valid ballots were processed in the first RCV round. The top five candidates were separated by only 181 first-choice votes. The winner was finally determined in the 20th RCV round, winning by only 442 votes of the 8200 continuing ballots.[84] By the 20th round, 4977 ballots (28%) were exhausted with less than 3 valid choices; however, 4631 ballots[85] (26%) were exhausted with three valid choices. It is highly conceivable that enough of the 4631 voters whose ballots were exhausted due to the 3-choice limit would have wanted to express more than 3 choices, and—given the spread of votes throughout the RCV elimination rounds—this expression could very well have changed the outcome of the election.

> **Finding 3:** San Francisco's Charter states that voters should be able to rank a number of choices in order of preference equal to the total number of candidates in an RCV race but may be limited to as few as 3 choices should it be infeasible, which it currently is due to

[83]U.S. Courts for the 9th Circuit government website, "Court of Appeals: Dudum v. Arntz, No 10-17198, May 20, 2011" (p. 32); http://www.ca9.uscourts.gov/datastore/opinions/2011/05/20/10-17198.pdf.
[84]City and County of San Francisco Department of Elections website, "Official Ranked-Choice Results Report, November 2, 2010: Consolidated Statewide Direct Primary Election Board of Supervisors, District 10"; http://sfelections.org/results/20101102/data/d10.html.
[85]City and County of San Francisco government website, "Department of Elections, San Francisco 2010 District 10: Table of Involuntarily Exhausted Ballots" (pdf file produced by David Cary for the VSTF); http://www.sfgov2.org/Modules/ShowDocument.aspx?documentid=461.

San Francisco's existing Sequoia voting system. This "restricted IRV" has been determined not to be a violation of a voter's constitutional right to vote. It does, however, impair the ability of the voter to fully express their preferences for candidates and such full expression of choices could change the outcome of RCV elections.

2.4.4 Recommendations

2.4.4.1 Public Understanding of RCV

1. San Francisco should reenergize its voter outreach and education efforts on RCV to better assure that voters have a good understanding of how votes are to be cast and counted. The Board of Supervisors should work with the Department of Elections to identify options and resources for renewed education efforts as soon as possible—preferably in advance of the November 2011 RCV elections. DOE has good, existing materials, and social networking sites such as Facebook and You Tube could offer an opportunity for low cost, high impact outreach. The VSTF encourages the Supervisors themselves to assist in public outreach to individuals and organizations in their districts.

2.4.4.2 Reporting Preliminary Early Election Results

2. Continue to release preliminary results for RCV contests as frequently as they are released for non-RCV contests. Include the full RCV algorithm and the supporting detail cast vote records (aka "ballot images") as part of preliminary results.
3. Implement Recommendation 2 to the extent feasible with the current system. Make this capability a requirement for any system to be acquired by San Francisco in the future.
4. Assure that RCV public awareness, outreach, and education includes the information on what interim result reporting information is available as well as how to access it and use it to track and understand the RCV election process and results.

2.4.4.3 Three-Choice Limit

5. Explore the possibility of increasing the number of choices with the existing Sequoia voting system. Make the ability to rank more than three choices a strong preference for any future voting system to be acquired by San Francisco with a preference for a system that will allow the voter to rank all candidates in a race.

2.5 Acquisition Strategies

2.5.1 Introduction

This section considers the voting systems "marketplace," including the state and federal regulatory/certification environment, economic considerations, and models for acquiring or developing a next generation system. It examines obstacles to innovation as well as potential partnership approaches that could break through existing barriers. It examines legal licensing options, including (1) proprietary, (2) disclosed, and (3) open source software and hardware approaches. It also puts forth software best practices that should be adopted regardless of the development strategy selected.

2.5.2. Concepts and Definitions

Public domain license: the class of license that is not limited by copyright and therefore essentially has no single owner to grant licenses. Since the work is not protected by copyright, it can be used, modified, and distributed by anyone without limitation.

Open source software: a range of concepts—such as software development practices—along with licensing rules. In this document we are using the Open Source Initiative (OSI) definition[86] of open source software; our focus is on licensing.

Disclosed source license: in this document, refers to a license that gives the licensee permission to review all source code—including that of firm-ware—and the ability to share all source code with other parties. All requestors should be able to run the code for testing purposes. No one should be restricted from publishing his/her findings. The code, however, can have a proprietary license that would restrict some rights; for example, the copyright owners could require a fee to run the code in production.

2.5.3 Findings

2.5.3.1 Regulatory/Certification Environment

The existing regulatory environment offers significant barriers to innovation. The certification process is shifting and cumbersome; it is extremely costly and time-consuming to bring a voting system through existing regulatory channels.

[86]Note: For the complete OSI definition for "open source software" that the VSTF is using, see http://opensource.org/docs/osd.

The State of California requires both state certification and federal certification by the U.S. Elections Assistance Commission (EAC) before a direct-record election device (DRE) can be used by a jurisdiction.[87] Testing is done by voting system test laboratories, which are labs accredited by the EAC.[88]

In the federal certification process, any modification to a voting system requires a re-testing of the entire system, even if the change is to an isolated part of the system. Therefore, even a small change to a voting system (such as a fix of a software defect) requires a very significant investment to achieve re-certification under the federal process. Estimates on the cost of federal certification vary; however, most estimates are in the range of $3-4 million dollars. Only six voting systems have been certified by the EAC. Congress is currently considering a proposal to dissolve the EAC, further contributing to lack of certainty about the future regulatory environment.

The following are some of the requirements for a new voting system to be certified by the Secretary of State in California:[89]

- Review of the application and documentation of the system
- End-to-end functional examination and testing of the system
- Volume testing under election-like conditions of the system and/or all voting devices with which the voter directly interacts
- Security testing that includes a full source code review and penetration (red-team) testing of the system
- Accessibility examination and testing of the system
- Public hearing and public comment period

The VSTF interviewed several Bay Area registrars as part of its research for this report, and all identified the regulatory process as a significant barrier to innovation/expansion of the marketplace.

Finding 1: The existing regulatory environment creates obstacles to innovation in voting systems.

2.5.3.2 Business and Partnership Models

The voting systems industry today is highly concentrated, and there are many barriers to entry: regulatory/certification barriers (as described in the previous section); a fragmented marketplace with varying systems requirements; and high development costs.

[87] See http://www.sos.ca.gov/voting-systems/cert-and-approval/vsysapproval/vs-conditions.htm.
[88] See http://www.eac.gov/testing_and_certification/testing_and_certification_program.aspx.
[89] California Secretary of State Debra Bowen government website, "Requirements of New Voting Systems"; http://www.sos.ca.gov/voting-systems/cert-and-approval/vsysapproval/vs-conditions.htm.

Currently, the State of California does not have consistent voting systems requirements across its 58 counties. Each jurisdiction must initiate an independent process for establishing its needs and must negotiate independently with private vendors to acquire a voting system that satisfies those needs. While it might be preferable for the State of California (i.e. the California Secretary of State) to develop statewide voting systems requirements, no such effort is currently envisioned.

Therefore, today the dominant model for implementing elections is for jurisdictions to purchase or lease proprietary voting systems from commercial vendors (see Sample Model A below). While this is currently the prevailing course of action, other models for acquiring a voting system warrant examination. Each possible approach brings a different set of economic and partnership considerations.

A range of sample models includes the following:

A. Purchase a Commercial Off-The-Shelf (COTS) Voting System
A jurisdiction purchases a voting system (equipment and services) from a private vendor that funded its development and certification. The code is proprietary and owned by the vendor. San Francisco employs this model with Sequoia Voting Systems.

B. Engineer to Order (Vendor Developed or Self-Developed)
A jurisdiction establishes system requirements and either uses a Request for Proposals (process to select a vendor to build the voting system) or employs a full development team to build the voting system. In either case the jurisdiction owns the system. The voting system may be based on existing software components or may be built entirely from scratch. The jurisdiction funds the costs of development and certification.

C. Public Partnership
Jurisdictions with similar systems and regulatory requirements partner and share resources to build and maintain a voting system. The jurisdictions pool their resources to fund the costs of development and certification.

D. Public/Private Partnership
A jurisdiction seeks partners that may include academic institutions, non-profits, other government entities, or even private sector technology companies willing to produce non-proprietary components. Based on system requirements, the consortium develops the code and component parts. However, the code is not proprietary and the jurisdiction either owns the code outright or has the ability to make modifications. The potential funding for this model could vary greatly depending on the specific solution, but it could include a combination of money from jurisdictions and from donors/volunteers.

There are existing non-profits that are building open source voting systems that are in various stages of readiness for elections. Two such organizations are the Open Voting Consortium (OVC) and Open Source Digital Voting Foundation (OSDV). There are also myriad systems that have been built by individuals and groups at academic institutions. Although many were built for specific research purposes and aren't made to be extended, some have the potential to be the

basis for full voting systems. The Caltech/MIT Voting Technology Project[90] is a good source of information on existing systems.

Los Angeles County is engaged in a robust effort (the Voting Systems Assessment Project or VSAP) to modernize its voting systems and is considering a variety of models/partnerships (including public/private partnerships) to acquire or develop such a system. Its goal, presented in the VSAP Incremental Plan,[91] is to have a new system in place by the end of 2015. Los Angeles is the largest and most diverse voting jurisdiction in the nation with 4.5 million registered voters. While the outcome of their VSAP is unknown and while San Francisco's needs will differ from those of Los Angeles County, their comprehensive effort has the potential to pioneer new approaches that might bring innovation to this stagnant marketplace.

Closer to home, Alameda County shares similar systems requirements with San Francisco, notably Ranked-Choice Voting.

It should be noted that, while all of the Bay Area registrars interviewed for this report were open to innovation in the voting systems marketplace, they expressed concern about the complexity of developing future voting systems using new acquisition models and getting them certified via the existing regulatory process.

> **Finding 2:** While there are barriers to moving away from the dominant model of purchasing a voting system from a private vendor, other acquisition models are possible and are being actively considered by other jurisdictions.

2.5.3.3 Transparency, Source-Code Disclosure, Licensing, and Contingency Planning

Sequoia Voting Systems developed San Francisco's current voting system using the company's proprietary system design and software development methodologies. The source code has been reviewed by some voting experts (through the California Secretary of State's 2007 Top-to-Bottom Review) and regulators, but the majority of the system is not open source and is not available for the general public to inspect. This makes it difficult for voters to establish confidence that the software is free of unknown software defects or design flaws. It is difficult to replace any aspect of the current voting system because the code is neither open source nor designed with clear modules.

The ability to review source code and systems design is an essential property of a trustworthy voting system. By giving the public access to the source code of a voting system, there is an increased chance that a defect will be found in a voting system, whether by the election

[90] CalTech/MIT Voting Technology Project, last accessed on June 23, 2011; http://vote.caltech.edu/drupal/.
[91] See http://www.lavote.net/General/PDFS/BOARD_CORRESPONDENCE/01272011-054459.pdf.

administrator or a member of the public. In his paper, Hall includes ideas for contingency plans to address possible discoveries.[92]

> **Finding 3:** Public review of source code increases the chance that defects will be identified and addressed.

2.5.3.4 Innovation

Although many jurisdictions have expressed interest in using alternative voting systems, most have not been able to go beyond researching and reporting on alternatives. Running a county-wide election is very complex, so it can be risky to try out new technologies. Several jurisdictions have tried out innovative solutions by initially testing redundant systems in limited ways in order to independently verify the accuracy of election results from the jurisdiction's proprietary voting systems.

Innovation can be done incrementally—it does not require a new elections system to be implemented and can be achieved with innovative processes in addition to technologies. For example, San Francisco is planning to open voting locations on Saturdays in the November 2011 election if the cost can be covered by private donations.[93] This is an innovation that has the potential to increase voter turnout without requiring any new technologies.

While this section has primarily discussed innovation for a jurisdiction's official results, there are several innovations for independently confirming the results of a jurisdiction's official system. One example is Takoma Park, Maryland, which used an open source system called Scantegrity in a municipal election (e.g. an election with no state or federal races).[94] Another is Humboldt County, California, that has used a project called the Humboldt County Election Transparency Project,[95] discussed in detail in Section 2.1: Election Records and Post-Election Audit.

> **Finding 4:** Innovation is possible even in conjunction with existing systems, but redundant methods of verifying the election result should be implemented whenever new innovations are tested.

2.5.3.5 Software Best Practices

There are standard software engineering best practices that have been found to create more reliable, maintainable software irrespective of the precise software development methodology used.[96] These include making sure code has ample unit-tests and is built using well-defined modules. An open source license does not ensure that code is high quality, so it is important to

---

[92]Hall, Joseph (2006), "Transparency Access to Source Code in Electronic Voting" (unpublished paper). http://josephhall.org/papers/jhall_evt06.pdf.
[93]See http://www.sfgov2.org/index.aspx?page=2390 for details.
[94]See http://www.scantegrity.org/takoma/ for details on how Scantegrity was used in Takoma Park, MD.
[95]See http://humtp.com/.
[96]For a comprehensive overview of best practices, see http://www.ibm.com/developerworks/websphere/library/techarticles/0306_perks/perks2.html.

make sure that any voting system under consideration has been built using best practices that have been accepted across the software industry.

2.5.4 Recommendations

2.5.4.1 Regulatory/Certification Environment

1. San Francisco should advocate with the California Secretary of State and the State legislature for a new, comprehensive state certification process to replace the existing requirement for federal certification. The state should aspire to a certification process that is more agile, efficient, and cost effective to enable innovation. The new state certification process should be sound enough to ensure that any new voting system would still meet the minimum federal requirements.

2.5.4.2 Business and Partnership Models

2. The VSTF supports the stated intention of the San Francisco Department of Elections (DOE) to renew its contract with Sequoia Voting Systems through 2013 with the stipulation that the short-term recommendations contained in this report—particularly concerning auditing—are implemented whenever feasible. We are also open to extending this contract through 2015 if doing so would allow San Francisco to take advantage of new technologies or partnership options that would be available in the middle term as a result of Los Angeles County's VSAP project. DOE should use the intervening period to consider a broad range of possibilities regarding the business and partnership model it will pursue to acquire/develop San Francisco's next voting system, including collaborating with other jurisdictions, academic institutions, or non-profit organizations.
3. To leverage its negotiating position, the DOE should consider reaching across the bay to Alameda County, which shares some similar requirements—notably Ranked-Choice Voting.
4. The DOE should take current academic research, including research on risk-limiting audits and end-to-end voting, into account to ensure that this work is considered in the selection of the City's next voting system.[97]
5. The DOE should closely monitor innovations in the voting systems vendor marketplace to determine if new products that meet the minimum requirements outlined in this report may be available in the required time frame.

[97]The Caltech/MIT Voting Project (http://vote.caltech.edu/) is a good resource for current academic research.

2.5.4.3 Transparency, Source Code Disclosure, Licensing, and Contingency Planning

6. The DOE should give strong preference to a voting system licensing structure that gives San Francisco all of the rights provided by an OSI-approved license,[98] even if the system is maintained by an external party.

   If an open source model is used, we recommend that the City of San Francisco work with other jurisdictions and organizations to develop and manage the code-base in order to leverage additional resources and expertise. The City of San Francisco should participate during the requirements gathering stage of development so that its unique requirements can be incorporated into the system design and implementation.

   If circumstances dictate that a solution that provides an OSI-approved license cannot be implemented by the time the contract for the City's current system expires, San Francisco should purchase voting equipment and services from a vendor who will provide a system that moves toward the following goals, irrespective of the other details of the license, so that any member of the public can perform the following tasks:

   - Review the source code of the entire system
   - Run code for testing
   - Distribute changes to code (i.e. documentation on defects and defect fixes can be distributed openly)

7. The DOE should set up a contingency plan in case a defect is found in the source code of the voting system. The contingency plan should include a volunteer committee of experts that can rapidly address any discovered defects and recommend procedures that can address those defects. The committee of experts should include computer scientists with expertise in voting systems and security and members of the DOE with deep knowledge on the voting systems and procedures in San Francisco.
8. San Francisco should be an active participant in the movement toward more open and transparent voting systems. We acknowledge the complexity of moving from the existing marketplace toward more innovative voting systems and urge San Francisco to move steadily toward the goal of transparency—even if it must do so in incremental steps. We encourage the City to be a strong advocate in the private sector marketplace for more transparent systems and to be open as well to new collaborative development models.

2.5.4.4 Innovation

9. It should be the policy of San Francisco to conduct pilot projects of alternative election technologies and procedures in municipal elections. This could initially involve a small number of precincts. These pilot projects would provide opportunities to learn how well alternative approaches work, such as using open source systems and hand counting paper

[98] For an alphabetical list of OSI-approved licenses, see http://www.opensource.org/licenses/alphabetical.

ballots at the polling places. All results of a pilot project should be confirmed using hand-counting.

2.5.4.5 Software Best Practices

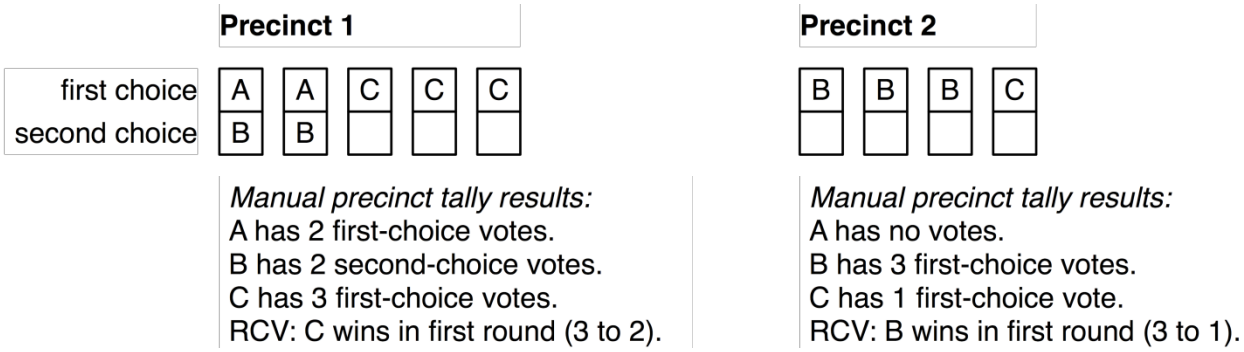
10. All voting systems software should be designed and implemented using the following modern, high-quality industry methodologies:

    a. Peer reviews of source code should be done throughout development of the new voting system.
    b. All source code should include extensive unit tests.
    c. The system should be modular in design with open data formats for exchanging data.
    d. There should be well-documented code, a clear technical architecture, and a detailed database design.
    e. The system should be delivered with extensive administrative (i.e. election workers) and end-user documentation (e.g. how system will be used by voters, including voters with different accessibility requirements).

Section 3: Appendices

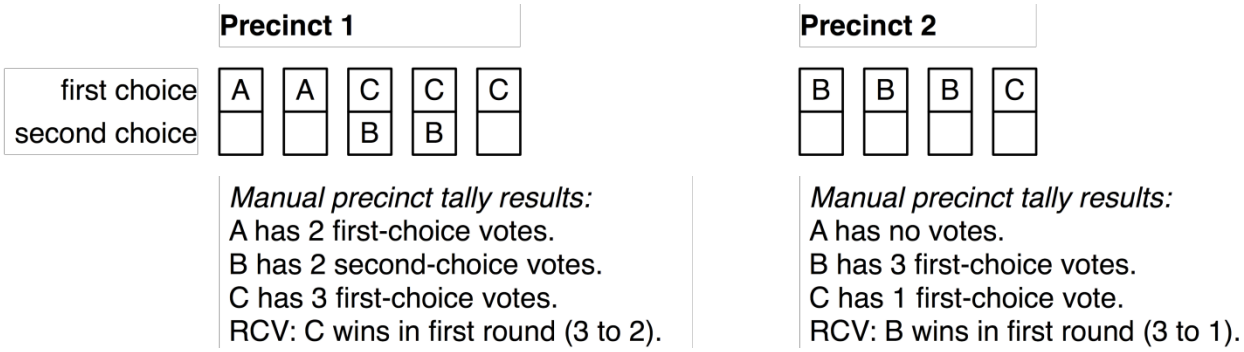
3.1 Appendix A: San Francisco's RCV Manual Tally Process

This appendix shows that the RCV manual tally process currently used in San Francisco does not audit the outcome of an election. Consider the following example of an RCV contest with three candidates (A, B, and C) and two precincts (5 ballots in Precinct 1, and 4 ballots in Precinct 2):



When all 9 ballots are counted together, no candidate has a majority of first-choice votes. Candidate A is eliminated, transferring 2 votes to Candidate B. In the second round of counting, Candidate B now has a majority (5 out of 9 votes) and wins the election.

Compare this to an alternate scenario with slightly different votes cast:



When all 9 ballots are counted together, again no candidate has a majority of first-choice votes, and Candidate A is eliminated. In the second round of counting, Candidate C now has a majority (4 out of 7 votes) and wins the election.

Notice that in both scenarios, manual tallies *within each precinct* produce exactly the same results. The total number of first-choice and second-choice votes for each candidate is the same. The RCV procedure, carried out within each precinct, produces the same result. So, even a 100% manual tally, using the current procedure, cannot distinguish these two scenarios—yet they yield different winners. This demonstrates that the current manual tally procedure does not correctly assure the RCV election outcome.

3.2 Appendix B: Summary of Outreach

In addition to welcoming public comment at its regular public meetings, the Voting Systems Task Force conducted the following research and outreach:

- Roger Donaldson and Jody Sanford met with John Arntz, Director of the Department of Elections for the City and County of San Francisco. (Fall 2009)
- Roger Donaldson, Jim Soper, and Ka-Ping Yee met with Lowell Finley, California Deputy Secretary of State. (9 October 2009)
- VSTF member Roger Donaldson (with Jim Soper) organized and attended a demonstration of the Prime III voting system (http://www.primevotingsystem.com) created by Dr. Juan Gilbert of Clemson University. This system is designed to address accessibility issues of concern to the disabled. (January 2010)
- A public comment period on "Draft VSTF Recommendations Under Consideration" document was held. (February 2010)
- Roger Donaldson (by phone) and Ka-Ping Yee met with San Francisco DOE staff members Nataliya Kuzina and Crispin Tirso on post-election audit procedures. (23 July 2010)
- VSTF members organized and attended a demonstration of the Trachtenberg Election Verification System (http://www.tevsystems.com) at San Francisco City Hall. (15 September 2010)
- Roger Donaldson, Ka-Ping Yee, and Jody Sanford met with Richard Matthews, Commissioner, San Francisco Elections Commission. (November 2010)
- Beth Mazur and Jody Sanford met with Dave MacDonald, Alameda County Registrar/Chief Information Officer. (27 January 2011)
- A public comment period on "Draft Recommendations on Voting Systems for the City and County of San Francisco" document was held. (February/March 2011)
- Beth Mazur and Jody Sanford met with Elaine Ginnold, Marin County Registrar. (1 March 2011)
- Jim Soper and Jody Sanford met with Stephen Weir, Contra Costa Elections Clerk. (22 March 2011)

Section 4:
About the VSTF

4.1 Membership of the VSTF

The Voting Systems Task Force has seven members with backgrounds in good government, computer science/software development, and accommodations serving persons with disabilities. Members serve as individuals and represent no other organization or group. The VSTF members are:

Jody Sanford, Chair
Ka-Ping Yee, Vice-Chair
Roger Donaldson
Tim Mayer
Beth Mazur
Gregory Miller
Jim Soper

Further information about the VSTF can be found at www.sfgov.org/vstf.

4.2 Biographies of VSTF Members

Roger Donaldson is currently a senior director at the Oracle Corporation where he has been employed since 1995. He began working on elections integrity and voting systems issues as a monitor with Election Protection during the 2004 Presidential election. He has served in nine San Francisco elections as a precinct inspector and field election deputy working for the San Francisco Department of Elections. He holds a Bachelor's degree in Economics and a Master's degree in Public Administration from the University of Southern California, and a Certificate in Government Contracts Administration from the University of California Los Angeles.

Tim Mayer is CEO of a business services company in San Francisco. He began his voter advocacy work in 2006. He has met with numerous county registrars and various voter advocacy groups, and he attended many government and private research and information meetings. He has observed and participated in precinct and county Election Day activities. Tim has observed several demonstrations of prototypical election systems developed by both for-profit and non-profit organizations. In 2008 he participated in the Open Voting Consortium[99] demonstration of open source/paper ballot printing voting systems developed by, amongst others, VSTF member Ka-Ping Yee.

[99] See http://www.openvotingconsortium.org/.

Beth Mazur is a technology consultant with extensive experience in open-source software and product management. She has held consulting and Product Management positions at a variety of software companies and non-profit organizations including Jaspersoft and Grameen Foundation. She has a longstanding interest in the use of technology for the improvement of the U.S. political process. Beth holds a Bachelor's of Science in Computer Science and Electrical Engineering from MIT.

Gregory Miller is the CEO for the Open Source Digital Voting Foundation. He has 28 years of technical and business experience in development and eventual commercialization of the Internet. He is a trained computer scientist with graduate business education and a law degree focused on intellectual property, technology law, and public policy. He is also active in the American Bar Association addressing technology law and public policy issues—including Cyberlaw, Information Privacy & Security, and Internet Governance. Greg is a member of the Congressional Internet Caucus Advisory Committee and a sustaining member of the Internet Society.

Jody Sanford served on the Board of the League of Women Voters of San Francisco from 2004 to 2009 and was its president from 2005 to 2007. She is a communications manager with the Presidio Trust, the agency leading the transformation of the Presidio of San Francisco from a military post to an innovative urban national park.

Jim Soper is a senior software consultant and the author of CountedAsCast.com. He is a co-chair of the Voting Systems Task Force in Alameda County, California, and a member of the California Election Protection Network's steering committee. Jim has been active in programming since the 1980s and in election integrity issues since 2005.

Ka-Ping Yee received his Ph.D. in Computer Science at University of California, Berkeley, for research in usability, security, and electronic voting. He served as a source code reviewer on the California Secretary of State Debra Bowen's "Top-to-Bottom Review of Voting Systems" in 2007. His dissertation, "Building Reliable Voting Machine Software,"[100] examines issues of security and verifiability, and proposes simplification as the path toward high-assurance voting machines. Ka-Ping joined Google.org as a software engineer in 2008.

This Report was edited by Lisa McFarren, www.mcfarrenwritingandediting.com.

[100]See http://zesty.ca/voting.